

Computer Law Reporter

A MONTHLY JOURNAL OF COMPUTER LAW AND PRACTICE

Publisher:
Neil J. Cohen, Esq.

Volume 60, Number 2

Washington, D.C.

October 2014

HIGHLIGHTS

The most noteworthy decisions this month are the following:

- In *Gomez v. Campbell-Ewald Co.* No. 13-55486 (9th Cir. Sep. 19, 2014), in a case where the Navy hired an advertising agency to obtain recruitments and the agency hired a contractor to send unsolicited text messages, the Ninth Circuit reversed a District Court ruling that the agency was immune from liability because a defendant may be held vicariously liable for TCPA violations where the plaintiff establishes an agency relationship, as defined by federal common law, between the defendant and a third-party caller.
- In *In re Adobe Systems, Inc. Privacy Litigation*, 13-CV-05226-LHK (N.D. Cal., Sep. 4, 2014), in this consolidated action, plaintiffs seek injunctive and declaratory relief and restitution on behalf of a class of Adobe customers whose personal information was accessed by hackers during a breach of Adobe's servers. The Court reaffirmed a Ninth Circuit opinion to the effect that an imminent threat that hacked personal information will be misused is sufficient to provide Article III standing, even if the misuse is not absolutely certain to occur. Contrary to some other district courts, the Court did not read the Supreme Court's *Clapper* decision as holding that the threat of misuse of hacked data is generally insufficient to confer standing on plaintiffs whose data was taken but has not yet known to have been misused. The Court also held that a state law restitution claim could be brought here even though the named plaintiffs did not subscribe to all the Adobe services that are encompassed within the proposed class definition. With respect to most of the named plaintiffs, the Court denied the motion to dismiss in its entirety.

(continued on page 4)

Contents

Page

**WEBSITE MARKETING STATEMENTS:
THE ACHILLES' HEEL TO
CDA PROTECTION?6**

**IS TARGET LIABLE TO
CARD-ISSUING BANKS?9**

RECENT DECISIONS27

BEST OF THE BLOGS51

DOCUMENTS

Opinion, Gomez v. Campbell-Ewald Co.

*Opinion, In re Adobe Systems, Inc.
Privacy Litigation*

*Opinion, Ades v. Omni Hotels
Management Corp. (Doc. No. 80)*

*Opinion, Ades v. Omni Hotels
Management Group (Doc. No. 81)*

Opinion, Jung v. Chorus Music Studio

*Opinion, Remijas v. Neiman
Marcus Group, LLC*

Comments on Our Other Publications . . .

The *Bank and Corporate Governance Law Reporter* is a monthly publication designed to serve litigators. It includes opinions, briefs, and transcripts of oral arguments in key FIRREA, FIDICIA, and corporate governance cases. Subscribers receive articles on cutting-edge issues, analyses of cases in the context of prior law, and detailed indexes.

"The *Reporter* probes beneath the surface of reported opinions in major M&A cases and gives to the reader ready access to the cutting-edge arguments made by leading practitioners in the field. It is a critical tool for anyone seriously interested in staying one step ahead of developing legal trends in the area."

A. Gilchrist Sparks III
Morris, Nichols, Arsht & Tunnell

PRICE: \$4275/YEAR

Many lawyers have discovered that the *Chemical Waste Litigation Reporter* is the most effective and comprehensive publication to obtain, organize and digest the flurry of judicial opinions in Superfund and related insurance, toxic tort and commercial cases. No other service publishes the decisions, organizes them under issue headings, and analyzes them in the context of existing case law.

"We are very pleased with your reporter and believe that it provides a very useful tool both in litigation and counseling clients in the area of hazardous waste."

Charles Tisdale, Jr.
King & Spalding

"The *Reporter* is an invaluable blend of published cases, briefs, news and analysis on the cutting edge of hazardous waste litigation. This publication is also a valuable research tool. Its well-organized index of relevant CERCLA provisions allows rapid identification of cases on point."

Michael A. Brown
McCutchen, Doyle, Brown & Enersen

PRICE: \$3775/YEAR

Many lawyers believe that the *RICO and Securities Fraud Law Reporter* is the most effective and comprehensive of the civil RICO reporting services. No other service publishes the decisions, organizes them under issue headings, and analyzes significant new decisions in the context of existing case law. Such headings include Arbitration, Burden of Proof, Conspiracy, Discovery, Enterprise, Equitable Relief, Evidence, Forfeiture/Disgorgement, Jurisdiction, Pattern, Pleadings, Predicate Acts, Res Judicata, Sanctions, and Standing. Also included every six months is a Cumulative Decision Index.

"The *RICO and Securities Fraud Law Reporter* is more than a 200-page monthly legal newsletter. By continuously publishing timely articles and analyzing and synthesizing the published opinions, the editors have created, in effect, a first-rate civil RICO treatise, updated monthly."

Frank C. Razzano
Pepper Hamilton LLP

PRICE: \$3725/YEAR

To order, call 202-462-5755

Visit us on the Web at <http://www.lawreporters.com>

Board of Editors

Fred M. Greguras, Esq.

K&L Gates
630 Hansen Way
Palo Alto, CA 94304

Tobey B. Marzouk, Esq.

Marzouk & Parry
1120 19th Street, N.W.
Seventh Floor
Washington, DC 20036-3605

Michael F. Mason, Esq.

Hogan & Hartson
555 13th Street, N.W.
Washington, DC 20004-1109

Gary J. Rinkerman, Esq.

Drinker, Biddle, & Reath LLP
1500 K Street, NW
Washington, DC 20005

Professor Stephen Saxby

Faculty of Law
Southampton University
Highfield, Southampton
S017 1BJ U.K.

Richard H. Stern, Esq.

Kellogg Huber Hansen
Todd, Evans & Figel, PLLC
1615 M Street, NW
Suite 400
Washington, DC 20036

J.T. Westermeier, Esq.

Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
11955 Freedom Drive
8th Floor
Reston, VA 20190-5675

E. Robert Yoches, Esq.

Finnegan, Henderson, Farabow,
Garrett & Dunner, LLP
1300 I Street, N.W.
Washington, DC 20005-3315

- In *Ades v. Omni Hotels Management Corp.*, No. 2:13-cv-02468-CAS(MANx) (Doc No. 80) (C.D. Cal. Sep. 8, 2014), in this case involving callers to a toll-free phone number whose calls allegedly were recorded without their consent, the Court granted the motion for class certification, holding that the class was reasonably ascertainable and the requirements of Federal Rule 23 had been met. The Court explained that a class action was superior to individual suits because it was unclear that the statutory damages available under the California Invasion of Privacy Act would incentivize individual actions. The Court also suggested that the possibility that an aggregate damages award for the class would be massive and raise Due Process/proportionality concerns was not a proper consideration at the class certification stage and should not preclude certification, particularly given that the California legislature had expressly adopted and retained \$5,000 as the minimum statutory damages for each violation of CIPA.
- In *Ades v. Omni Hotels Management Group*, No. 2:13-CV-2468-CAS(MANx) (Doc. No. 81) (C.D. Cal. Sep. 8, 2014), in this class action lawsuit seeking statutory damages under the California Invasion of Privacy Act (CIPA) based on the alleged recording of customer calls without consent, the Court denied the defendants' motion for summary judgment. The Court held that California law applied even though the call center was located in Nebraska. The Court also held that application of CIPA to calls made by Californians to the call center in Nebraska did not violate the Dormant Commerce Clause. The Court explained that there was a triable issue as to whether the call center could identify the state of origin of callers, and hence could treat calls from California differently from calls from other states. The Court also suggested that even if CIPA incentivized national call centers to comply with CIPA with respect to *all* incoming calls, CIPA did not necessarily violate the Dormant Commerce Clause. Indeed, CIPA did not in any way represent extraterritorial regulation. The Court also found no merit in defendants' other arguments for summary judgment.
- In *Jung v. Chorus Music Studio*, No. 13-CV-1494 (CM)(RLE) (S.D. N.Y. Sep. 11, 2014), the Courts of Appeals are split as to whether the Computer Fraud and Abuse Act (CFAA) creates liability whenever an employee misuses a workplace computer by using information contained on it for improper purposes or whether, more narrowly, it creates liability only when the employee accessed a computer that he or she was altogether prohibited from using. In opposing the filing of a CFAA counterclaim as futile, the plaintiffs in this case argued that the Second Circuit had embraced the narrow view of the CFAA as creating liability only for unauthorized access to an employer's computer. The Court, however, read the Second Circuit precedent as inconclusive on this issue and allowed the proposed counterclaim to be filed against a named plaintiff who was authorized to use the

computer at issue but who allegedly misused the information he found on it for his own personal business venture. The Court thus suggested that it may agree with the broad view of the CFAA as creating liability for misuse of employer information, although the Court did not squarely rule on that issue in this opinion.

- In *Remijas v. Neiman Marcus Group, LLC*, No. 14 C 1735 (N.D. Ill. Sep. 16, 2014), the Court held that department store customers whose credit card information was or may have been stolen lacked standing to sue the department store. Even with respect to those customers whose data actually was stolen and who had fraudulent charges made to their credit cards, there was an insufficiently concrete injury for Article III standing, because those customers presumably had those fraudulent charges removed from their accounts and were not forced to pay them. The time and effort dealing with fraudulent charges was dismissed by the Court as de minimis and insufficient to qualify as a concrete injury. The Court also was unpersuaded by the plaintiffs’ “creative” theory that they overpaid for the defendants’ products because the prices for those products should have included defendant’s costs of providing adequate data security, which in fact was not provided. The Court did hint that more specific allegations of harm from incurring fraudulent charges on the part of individual plaintiffs might be sufficient to establish standing.

Website Marketing Statements: The Achilles' Heel to CDA Protection?

Jeffrey D. Neuburger*

It's no secret that local directory/consumer review websites are popular among consumers looking for recommendations before dining out, hiring a contractor, or even picking a dentist or day spa. Yelp reported around 138 million monthly unique visitors in the second quarter of 2014, searching among over 61 million local reviews. The bottom line is that solid reviews and multiple stars on local search sites can drive sales; on the other hand, and to the chagrin of business owners, low ratings and a spate of one-star rants displayed prominently at the top of a listing can drive customers away.

Review sites typically have to wrestle with the problem of unreliable or fictitious reviews, which are blurbs written by friends or employees of the listed business, paid reviews, and negative reviews written by business competitors. Some sites use filtering software to identify and remove unreliable reviews – of course, such software is not perfect, and businesses have complained that some sites have filtered out legitimate reviews, but left in other fake reviews to the detriment of the reviewed businesses.

A number of businesses have brought suit against consumer review sites claiming that they purposely remove positive reviews (but leave up defamatory complaints), arbitrarily reorder the appearance of reviews, or otherwise wrongfully tinker with the algorithms that are supposed to weed out “fake” reviews presumably to encourage or “extort” businesses to purchase advertising or pay for additional features.

Most suits that have sought to hold sites responsible for defamatory content created by third-party users have been rejected by courts based upon CDA Section 230, which immunizes “interactive computer services” – such as a consumer review websites – where liability hinges on content independently created or developed by third-party users.

To get around the broad immunity, some businesses have urged courts to interpret an intent-based exception into Section 230, whereby the same conduct that would otherwise be immune under the statute (e.g., editorial decisions such as whether to publish or de-publish a particular review) would be actionable when motivated by an improper reason, such as to pressure businesses to advertise. However, several courts have rejected this theory.

* Jeffrey D. Neuburger is a partner with Proskauer Rose LLP and Co-Chair of Technology, Media & Communications for the firm. This article originally appeared on the firm's blog at newmedialaw.proskauer.com. Copyright © Proskauer Rose LLP. Reprinted by permission.

- *Reit v. Yelp!, Inc.*, 29 Misc 3d 713 (N.Y. Sup. Ct. 2010) (Yelp’s selection of the posts it maintains on its site can be considered the selection of material for publication, an action “quintessentially related to a publisher’s role,” and therefore protected by CDA immunity)
- *Levitt v. Yelp! Inc.*, 2011 WL 5079526 (N.D. Cal. Oct. 26, 2011) (our prior post on the *Levitt* opinion) (CDA Section 230 contains no explicit exception for impermissible editorial motive, particularly since traditional editorial functions often include subjective judgments that would be “problematic” to uncover, thereby creating a chilling effect on online speech that Congress sought to avoid). Note, on appeal, the Ninth Circuit affirmed the district court’s dismissal of the plaintiffs’ claims – though not on the basis of CDA Section 230 – alleging Yelp extorted advertising payments from them by purportedly manipulating user reviews.
- *Kimzey v. Yelp Inc.*, 2014 WL 1805551 (W.D. Wash. May 7, 2014) (mere fact that an interactive computer service “classifies” user characteristics and displays a “star rating system” that aggregates consumer reviews does not transform it into a developer of the underlying user-generated information).

However, in recent disputes, businesses have sought an end run around CDA Section 230, specifically by bringing claims that do not treat the websites as publishers or speakers of the defamatory or fictitious user reviews, but instead relate to the website’s marketing representations about such content. At least two courts have allowed such claims to go forward, bypassing CDA immunity.

In one such case, *Moving and Storage, Inc. v. Panayotov*, 2014 WL 949830 (D. Mass. Mar. 12, 2014), the plaintiffs alleged that a moving company review website (that itself was operated by a moving company) intentionally deleted positive reviews of the plaintiffs’ companies and deleted negative reviews that criticized its own company to gain market share, all the while representing that the site offered “the most accurate and up to date rating information.” The court concluded that CDA Section 230 did not bar plaintiffs’ false advertising and unfair competition claims because they were not based on information provided by “another information content provider,” and did not arise from the content of the reviews.

Most recently, a California appellate court reversed a lower court’s dismissal of an action against Yelp over alleged false advertising regarding its automated review filter. In *Demetriades v. Yelp, Inc.*, 2014 WL 3661491 (Cal. App. July 24, 2014), the plaintiff brought state law claims for unfair competition and false advertising alleging that Yelp engaged in false advertising based upon marketing statements stating that user reviews passed

through a filter that gave consumers “the most trusted reviews” and only “suppresse[d] a small portion of reviews.”

The plaintiff alleged that Yelp’s statements about its filtering practices were misleading because its filter suppressed a substantial portion of reviews that were trustworthy and favored posts of the “most entertaining” reviews, regardless of the source. The lower court had previously granted Yelp’s motion to strike the plaintiff’s complaint under California’s anti-SLAPP provisions, which aim to curb “lawsuits brought primarily to chill the valid exercise of the constitutional rights of freedom of speech and petition for the redress of grievances.” Cal. Code Civ. Pro. §425.16 (a). The appellate court reversed, holding that false advertising-like claims involving commercial speech fell outside the reach of the anti-SLAPP statute and that Yelp’s representations about its filtering software—as opposed to the content of the reviews themselves—were “commercial speech about the quality of its product.”

Regarding the application of CDA Section 230, the court rejected Yelp’s argument that plaintiff’s claims should be dismissed because courts have widely held that claims based on a website’s editorial decisions (publication, or failure to publish, certain third-party conduct) are barred by Section 230. In a brief paragraph, the appellate court stated that the CDA was inapplicable because the plaintiff was not seeking to hold Yelp liable for the statements of third-party reviewers, but rather for its own statements regarding the accuracy of its automated review filter.

Companies, frustrated with their portrayal on online review sites, have mostly struck out when seeking to hold website operators liable for managing and displaying user-generated reviews. However, this past year, some courts have offered companies another potential avenue at obtaining relief. While the courts merely allowed the claims related to marketing representations to survive dismissal at the early stages of litigation, it is uncertain how either court will rule on the merits.

With this in mind, sites that collect and manage user-generated content, or otherwise use automated filtering software to manage content, should examine marketing statements on their websites for any language that goes beyond mere puffery and might be construed as misleading.

Is Target Liable to Card-Issuing Banks?

Publisher's Introduction

Beginning on the next page is an amicus brief on behalf of internet companies seeking certiorari in the Supreme Court to overturn the Ninth Circuit's decision in *Spokeo v. Robbins*, holding that a statutory violation without damages is sufficient to confer Article III standing. The petitioners argue that there is a split in the Circuits and that enforcement of pure statutory rights should be left to the government.

Computer Law Reporter

1601 Connecticut Avenue, N.W., Suite 701, Washington, DC 20009 • 202-462-5755 • Fax 202-328-2430

UNITED STATES DISTRICT COURT DISTRICT OF MINNESOTA

In re: Target Corporation Customer Data
Security Breach Litigation

This Document Relates to: All

Financial Institution Cases

MDL No. 14-2522 (PAM/JJK)

Umpqua Bank, Mutual Bank, Village Bank,
CSE Federal Credit Union, and First Federal
Savings of Lorain, individually and on
behalf of a class of all similarly situated
financial institutions in the United States,

Plaintiffs,

vs.

Target Corporation,

Defendant.

TABLE OF CONTENTS

I.	SUMMARY OF PERTINENT FACTUAL ALLEGATIONS	1
A.	The Criminal Intrusion on Target's Computer Network	1
B.	The Parties and Their Roles in the Payment Card Networks	2
II.	SUMMARY OF THE ARGUMENT	3
III.	LEGAL STANDARD	4
IV.	ARGUMENT	5
A.	The Banks' Negligence Claim Must Be Dismissed	5
1.	The Banks Fail to Plead that Target Owed Them a Duty of Care	5
2.	The Banks' Allegations of Breach of Duty Fail to Satisfy <i>Iqbal</i> and <i>Twombly</i>	14
B.	The Banks' Claim For Negligent Misrepresentation by Omission Must Also Be Dismissed	16
1.	The Banks Fail to Allege that Target Owed Them a Duty of Care	17
2.	The Banks Fail to Allege Any Actionable Misrepresentation by Omission	21
3.	The Banks Have Failed to Allege Reliance	25
C.	The Banks' Claim For Violation of the Minnesota Plastic Card Security Act Must Be Dismissed	26
1.	The Banks Fail to Allege that Target Retained Any Payment Card Data in Violation of the Minnesota Plastic Card Security Act	26
2.	The Minnesota Plastic Card Security Act Only Applies to Business Conducted in Minnesota	29
D.	Because the Banks Have Failed to State a Claim For Violation of the Minnesota Plastic Card Security Act, They Have Likewise Failed to State a Claim For Negligence <i>Per Se</i> Based on that Act	30
V.	CONCLUSION	30

DEFENDANT'S MEMORANDUM OF LAW IN SUPPORT OF MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT

Target Corporation ("Target") submits this memorandum of law in support of its

Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint ("Complaint").

I. SUMMARY OF PERTINENT FACTUAL ALLEGATIONS

A. The Criminal Intrusion on Target's Computer Network.

On December 19, 2013, Target announced that it had been the victim of a criminal attack on its computer network by third-party intruders (the "Intrusion"), which had been confirmed only four days earlier. Compl. ¶ 68 n.2. The Intrusion was carried out by sophisticated criminal hackers (Compl. ¶ 103), who gained access to Target's network through credentials they stole from a third-party vendor whom Target retained for HVAC maintenance. Compl. ¶¶ 41, 46. Once inside the Target network, the hackers deployed custom point-of-sale malware to Target's registers, which collected credit and debit card (jointly, "payment card") information "in real time" when customers swiped their cards at Target registers between December 2, 2013 and December 15, 2013. Compl. ¶¶ 49, 56.

Target's security measures were certified by an independent auditor as compliant with "all payment industry requirements" and included "state of the art" tools that Target invested substantial resources to acquire. Compl. ¶¶ 28, 34, 44. However, plaintiffs – a group of five payment-card-issuing banks, credit unions, and savings associations (the "Banks") (Compl. ¶¶ 7–12) – nonetheless assert that Target is to blame for not preventing the Intrusion. Compl. ¶¶ 2, 86. They claim resulting financial losses that include costs associated with reissuing payment cards to customers and reimbursing fraudulent charges.

Id.

B. The Parties and Their Roles in the Payment Card Networks.

The Banks are headquartered in Oregon, Massachusetts, Minnesota, Louisiana, and Ohio. Compl. ¶¶ 7–12. Target is a Minnesota corporation with retail locations throughout the United States. Compl. ¶¶ 13–14.

Payment card issuers like the Banks participate in an "extensive network of financial institutions" that together process retail payment card transactions. Compl. ¶ 18. This process begins with a financial institution, like the Banks, issuing a payment card to a consumer. The consumer then may choose to use that payment card to make purchases at retail merchants, such as Target. Compl. ¶ 17. When this occurs, the merchant obtains authorization and payment for the transactions not from the bank that issued the card (the "issuing bank"), but rather from a payment processor and/or a merchant bank (an "acquiring bank") that has contracted with the merchant to handle the transaction. *Id.* The acquiring bank in turn obtains authorization and payment under its separate contract with a payment card company such as Visa and MasterCard (the "Card Brands"), and the Card Brand in turn obtains authorization and funding under its separate contract with the issuing bank.¹ Thus, issuing banks and merchants have no direct dealings with one another in the payment card transaction process.

¹ See Visa International Operating Regulations (Oct. 15, 2013), at *49, *51, *941, *1019 (Decl. of Douglas H. Meal ("Meal Decl."), Ex. A) (providing that acquirers and issuers are both "Members" who contract with Visa and are subject to Visa's Operating Regulations). Because the Card Operating Regulations are "necessarily embraced by the pleadings," see, e.g., Compl. ¶¶ 17–18, the Court may consider them on a motion to dismiss. *Twin City Sprinkler Fitters v. Total Fire Prot. Inc.*, No. Civ. 02-930 PAMRLE, 2002 WL 31898170, at *1 n.1 (D. Minn. Dec. 26, 2002). See also *Banknorth v. BJI's*

The Card Brands have issued comprehensive regulations governing these processes ("Card Operating Regulations"). Compl. ¶ 18. Although merchants do not contract directly with the Card Brands, the Banks allege that the Card Operating Regulations are incorporated into merchants' contracts with acquiring banks. *Id.* The Banks also allege that merchants are contractually bound to comply with the Payment Card Industry Data Security Standard ("PCI-DSS"), which sets forth information security requirements by the Payment Card Industry Security Standards Council, through an unspecified agreement. *Id.* ¶¶ 19, 129.

II. SUMMARY OF THE ARGUMENT

In their Complaint, the Banks assert counts for negligence (Compl. ¶¶ 100–11) and negligent misrepresentation by omission (Compl. ¶¶ 127–34), as well as for violation of the Minnesota Plastic Card Security Act (the "PCSA") (Compl. ¶¶ 112–20) and negligence *per se* based on the PCSA (Compl. ¶¶ 121–26). Each is fundamentally flawed.

The Banks' negligence and negligent misrepresentation claims hinge, among other things, on there being a never-before recognized "special relationship" between merchants, like Target, and payment card issuers, like the Banks, that justifies creation and imposition of a novel *common-law* duty of care. The Banks, however, are sophisticated parties that do not even have a *direct* relationship with Target, much less a *special* relationship that might suffice to create such a duty in either the negligence or negligent misrepresentation context. Especially since (i) the Minnesota Legislature

Wholesale Club, Inc., 442 F. Supp. 2d 206, 213 (M.D. Pa. 2006) (noting that issuing banks operate through a contract with a Card Brand).

already has addressed the issue of when a merchant might be liable to an issuer following a data breach; (ii) the contractual regime upon which the Banks base many of their claims *already* provides a system under which issuers may be compensated following a data breach; and (iii) courts in other jurisdictions *already* have refused to impose common-law tort duties based on similar allegations, the facts alleged here do not justify the imposition of new and unprecedented common-law tort duties under Minnesota law. Even if that were not the case, the Banks' failure to plead other elements of their claims, such as breach, an actionable misrepresentation by omission, or reliance, would nonetheless require dismissal.

In an attempt to plead around these fatal defects, the Banks resort to the PCSA and an accompanying negligence *per se* claim. But neither can save the Banks' Complaint, since the Banks' own allegations confirm that the intrusion involved theft of payment card data "in real time," and thus did not involve a PCSA violation.

III. LEGAL STANDARD

To withstand a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6), a plaintiff must proffer more than mere "labels and conclusions," but rather must allege sufficient factual matter to "raise a right to relief above the speculative level." *Peterson v. Argent Morig. Co.*, No. 06-3796, 2007 WL 1725355, at *1 (D. Minn. June 14, 2007) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)); *see also Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

IV. ARGUMENT

A. The Banks' Negligence Claim Must Be Dismissed.

Count I of the Complaint asserts a claim for negligence. To state a claim for negligence under Minnesota law,² a plaintiff must allege (1) the existence of a duty, (2) breach of that duty, (3) proximate cause, and (4) injury. *See, e.g., Johnson v. State*, 553 N.W.2d 40, 49 (Minn. 1996).

The Banks have failed to plead that Target owed the Banks any duty of care or that Target breached any such duty, the absence of either of which requires dismissal.

1. The Banks Fail to Plead that Target Owed Them a Duty of Care.

The existence of a duty of care is a threshold requirement for negligence – absent a legal duty, the Banks' claim fails. *See, e.g., id.* at 50. In the Complaint, the Banks variously allege that Target owed them a duty in “obtaining, retaining, securing, and deleting” payment card information that Target collects from its consumers, providing security for that information consistent with industry standards, and thwarting intrusions “routinely attempted” by “sophisticated hackers.” *See* Compl. ¶¶ 101–103, 106. No matter how the Banks cast their assertions of duty, however, they all boil down to the contention that a merchant has a *common-law* duty to take certain steps to protect issuing banks from financial losses caused by third-party criminal attacks aimed at stealing payment card data. Minnesota law recognizes no such duty.

² Because the Complaint nowhere purports to differentiate between the laws applicable to the five Banks' claims, Target assumes for purposes of this motion to dismiss, without conceding, that Minnesota law applies to all of the Banks' common-law claims.

“As a general rule, a person has no duty under Minnesota law to protect another from the harmful conduct, including criminal conduct, of a third person.” *RKL Landholding, LLC v. James*, No. A12-1739, 2013 WL 2149979, at *2 (Minn. Ct. App. May 20, 2013) (citing *Donaldson v. Young Women's Christian Ass'n of Duluth*, 539 N.W.2d 789, 792 (Minn. 1995)). This is so even when “an actor realizes or should realize that action on his part is necessary for another's aid or protection.” *Johnson*, 553 N.W.2d at 49. Instead, a duty to protect against third-party criminal harm arises only where (i) there is a special relationship between the defendant and the plaintiff (or the defendant and the third party); and (ii) the third-party harm is foreseeable. *Clark ex rel. H.B. v. Whittemore*, 552 N.W.2d 705, 707 (Minn. 1996). Here, the Court need not even reach the issue of foreseeability, because the Banks plead no facts in support of their conclusory assertion that “Target maintained a special relationship” with them (Compl. ¶ 104). *See Johnson*, 553 N.W.2d at 50 (holding that the court “need not reach the issue of foreseeability” where the plaintiffs failed to plead the requisite special relationship).³

³ Minnesota also recognizes that an actor owes a limited duty to protect another from its own misfeasance – i.e., “active misconduct working positive injury to others,” *see W. Page Keeton et al., Prosser and Keeton on the Law of Torts* § 56 (5th ed.1984); *see also Catlin Underwriting Agencies*, No. A13-2078, 2014 WL 3800595, at *5 (Minn. Ct. App. Aug. 4, 2014) – but the Complaint's assertions about “Target's own conduct” (Compl. ¶ 106) amount to nothing more than claims of nonfeasance: that Target failed to take steps that may have stopped the third-party criminal attackers from doing harm. *See BancFirst v. Dixie Rests., Inc.*, No. CIV-11-174-L, 2012 WL 12879, at *4 (W.D. Okla. Jan. 4, 2012) (allegations of a merchant's failure to prevent a data breach do not suffice as “affirmative acts”). Minnesota also recognizes that an actor may voluntarily undertake (or assume) a duty which otherwise does not lie, but only where plaintiff's allege property damage or personal injury. *See, e.g., United HealthCare Ins. Co. v. Advance PCS*, No. Civ.01-2310 (RIH/AJB), 2003 WL 22316555, at *4 (D. Minn. Oct. 6, 2003) (“Minnesota law . . . does not allow recovery for economic losses stemming from a

Minnesota courts recognize a special relationship only in a very narrow set of circumstances where the plaintiff's vulnerability and dependence or other public policy considerations require the imposition of special tort duties. *See Clark*, 552 N.W.2d at 709. The Minnesota Supreme Court has "carefully carved out" the following "as the outer boundaries" of special relationship categories: "common carriers, innkeepers, possessors of land who hold it open to the public, and persons who have custody of another person under circumstances in which that other person is deprived of normal opportunities of self-protection." *Id.*; *see also Johnson*, 553 N.W.2d at 49. Numerous decisions make clear that Minnesota courts are reluctant to extend special relationship duties beyond these categories. *See, e.g., Funchess v. Cecil Newman Corp.*, 632 N.W.2d 666, 674 (Minn. 2001); *RKL Landholding*, 2013 WL 2149979, at *2-3 ("[T]he 'special relationship' exception is a narrow one The supreme court has expressed reluctance to expand on the exceptions to the general rule.").

Plainly, none of these traditional categories applies here. The Banks instead seek the creation of a new special relationship between merchants and issuing banks based on the allegation that the Banks "entrusted Target with the personal and financial information of customers using credit and debit cards issued by [the Banks] on the premise that Target would safeguard this information. . . ." Compl. ¶ 104. In addition to falling well outside the "outer boundaries" delineated by the Minnesota Supreme Court, the creation of an issuing-bank/merchant special relationship would undermine the role of breach of an assumed duty." The Banks do not allege any voluntary undertaking here, nor do they allege property damage or personal injury. Thus, the Banks' inability to allege a special relationship is fatal to their claim.

the Minnesota Legislature and otherwise be flatly inconsistent with prevailing Minnesota law.

To the extent the general rule in Minnesota is that a court should be reluctant to recognize new special relationship duties in tort, such reluctance surely must be amplified where the state legislature has already promulgated legislation on the topic that stops short of imposing by *statute* the very duty a plaintiff claims already exists at common law. Here, the Banks assert that the PCSA supports their negligence count. Compl. ¶ 110. In fact, however, that statute only serves to underscore the *non-existence* of the common-law tort duty on which that count is based.

Through the PCSA, the Legislature could have required merchants to reimburse issuing banks for costs associated with *any* data breach that the merchant allegedly could have prevented. It did not. Instead, the PCSA carefully limits the circumstances in which a merchant might be required to reimburse an issuing bank, imposing liability *only* when the data breach involved the theft of certain types of sensitive payment card data that the merchant had been storing in violation of the statute. Minn. Stat. § 325E.64, subd. 2-3 (2013). Here, the Banks' own allegations regarding the operation of the attacker's malware make clear that the PCSA provides the Banks no cause of action against Target. *See infra*, at Part IV.C. In asking this Court to find that Target owed them a *common-law* duty to take certain steps to prevent the intrusion, then, the Banks are asking the Court to take the unprecedented step of imposing a common-law duty that goes above and beyond what the Legislature saw fit to impose. Target is not aware of any case in which a court found that a "special relationship" and accordingly a common-

law duty existed under Minnesota law in similar circumstances where the Minnesota Legislature had stopped short of statutorily imposing the duty in question. Courts in other data breach cases, however, have refused to create common-law duties beyond those enumerated by statute. *See Digital Fed. Credit Union v. Hannaford Bros. Co.*, No. BCD-CV-10-4, 2012 WL 1521479, at *3 & n.5 (Me. B.C.D. 2012) (rejecting issuing banks' attempts to impose "potentially unlimited liability" on merchants for a data breach, where the Maine Legislature limits a merchant's duty to notifying Maine residents of a breach); *Cooney v. Chi. Pub. Schs.*, 943 N.E.2d 23, 28-29 (Ill. App. Ct. 2010) (refusing to recognize a common-law duty to safeguard information where the Illinois Legislature requires only notice of a breach).

Even if the PCSA did not exist, this would not be an appropriate case for the Court to find that Target and the Banks had a "special relationship" such that Target had a common-law duty to protect the Banks from being injured by the criminal attack that Target suffered. As an initial matter, it does not appear that a Minnesota court ever has recognized a special relationship that requires one party to protect another from a third party's wrongful infliction of *economic* losses, as is alleged here. *See* Compl. ¶ 86. The distinction between third-party-inflicted economic losses on the one hand, and third-party-inflicted personal injury on the other, is consistent with the Minnesota Supreme Court's mandate that courts be reluctant to find new special relationships and has been noted in at least one decision as reason to reject claims of a special relationship. *See RKL Landholding*, 2013 WL 2149979, at *3 (no special relationship requiring contractor to protect owner's vacant building, in part because "there were no human occupants to

protect"). Moreover, even where grievous physical harm was alleged, Minnesota courts have found that policy considerations counsel against imposing tort duties requiring protection against criminal intruders. *See Finckhess*, 632 N.W.2d at 673 n.4, 675 (finding no special relationship between landlord and tenant who was murdered by an intruder, reasoning that crime prevention is the duty of the government, not businesses, and noting the unpredictability of criminals "bent on defeating security measures").

But perhaps most significantly, Minnesota courts consistently and repeatedly have held that commercial transactions do not give rise to a special relationship, because commercial actors are "not the types of parties deemed to be vulnerable that would require protection." *See, e.g., Superior Constr. Servs., Inc. v. Moore*, No. AO6-1491, 2007 WL 1816096, at *3 (Minn. Ct. App. June 26, 2007) (finding no special relationship between bank and a contractor, even though bank had custody and control of funds allegedly owed to contractor); *United Prods. Corp. of Am., Inc. v. Atlas Auto Parts, Inc.*, 529 N.W.2d 401, 403-04 (Minn. Ct. App. 1995) (finding no special relationship between neighboring businesses); *Mack v. Britto Cent., Inc.*, No. 13-197, 2013 U.S. Dist. LEXIS 110142, at *25 (D. Minn. Aug. 6, 2013) (dismissing negligence claim with prejudice where art dealer failed to plead a special relationship with artist and other art dealers); *superseded on other grounds*, 2014 WL 1608364 (D. Minn. Apr. 21, 2014).

Further, Minnesota courts are particularly unwilling to find a special relationship where, as here, a contractual scheme allocates (or could allocate) the parties' duties and risks. *See, e.g., RKL Landholding*, 2013 WL 2149979, at *3 (holding that if a property owner expected a contractor to protect the vacant building at issue, it "should have

obtained [contractor]'s agreement to do so.”). This principle is not peculiar to claims of a special relationship, but rather has been recognized by the Minnesota Supreme Court as a fundamental boundary between duties in contract and tort. *See Glorvigen v. Cirrus Design Corp.*, 816 N.W.2d 572, 584 (Minn. 2012) (holding that a plaintiff cannot recover in negligence when its claims are premised on a defendant’s allegedly having failed to comply with contractual duties); *see also M&I Marshall & Ilsley Bank v. Federated Mut. Ins. Co.*, No. 27-CV-10-15648, 2011 WL 2742950 (Minn. Dist. Ct. Feb. 2, 2011).

The Banks, as financial institutions that issue payment cards and participate in the complex networks required in order to process retail payment card transactions (Compl. ¶¶ 12, 17), are precisely the type of sophisticated commercial actors for which a special relationship will not be found, particularly since their negligence claim is premised on Target’s allegedly having failed to comply with “industry standards and requirements,” namely, the Card Operating Regulations and the PCI-DSS, which the Banks concede are enforceable on Target only as a result of Target’s contracts with third parties. Compl. ¶¶ 18–19, 102, *see also* Compl. ¶¶ 17–18, 22, 106–07. The Card Operating Regulations, moreover, include specific remedies available to issuing banks in the event of a breach at a participating merchant, as the Banks no doubt are aware. *See* Visa International Operating Regulations, at *676 (Meal Decl., Ex. A) (describing process by which an issuing bank “may recover a portion of its Incremental Counterfeit Fraud losses and operating expenses resulting from an Account Data Compromise Event” if the merchant at issue had not been compliant with the PCI-DSS); MasterCard Security Rules and Procedures, Merchant Edition (August 30, 2013), at §10.2.5.3 (Meal Decl., Ex. B)

(describing reimbursement process enabling “an Issuer to partially recover costs” incurred in reissuing cards, enhanced monitoring of accounts, and counterfeit fraud losses); *see also In re TJX Cos. Retail Sec. Breach Litig.*, 246 F.R.D. 389, 398–99 (D. Mass. 2007) (describing methodology Visa enacted “to provide an efficient and cost-effective method of settling disputes arising out of account data compromises and resultant fraud”). Having acknowledged that the Card Operating Regulations govern members’ participation in the card brand networks, the Banks cannot now seek to renegotiate these agreements and their remedies by asserting a claim in tort.

Finally, the allegations in the Complaint undermine the very assertion that *the Banks* “entrusted” anything to Target. *See* Compl. ¶ 104. The Banks repeatedly acknowledge that it was “the personal and financial information of *consumers*,” not the Banks, that allegedly was stolen (Compl. ¶¶ 104–105, 107 (emphasis added)), and that this information was provided to Target *by such consumers* (Compl. ¶ 17). Thus, the Complaint does not even allege a direct relationship between the parties. Insofar as Minnesota courts already have rejected the claim that “a mere merchant-customer relationship” gives rise to a duty to protect customers, *Superior Constr.*, 2007 WL 1816096, at *3 (no special relationship between bank and contractor for whom it allegedly was holding funds in escrow), Target cannot be found to have a special relationship with the Banks, who are one more step removed. *Cf. Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 851–52 (N.D. Cal. 2012) (finding no special relationship under California law between Apple and Apple customers alleging that Apple failed to protect customers’ information from third-party app developers).

Dismissal of the Banks' negligence claim because Target owed the Banks no duty is consistent with decisions dismissing similar claims asserted by issuing banks against merchants in other data breach cases. See *BancFirst v. Dixie Rests., Inc.*, No. CIV-11-174-L, 2012 WL 12879, at *4 (W.D. Okla. Jan. 4, 2012) (dismissing negligence claim under Oklahoma law against breached restaurant because there was no special relationship between the parties, noting the "attenuated" relationship between merchants and issuing banks and the fact that compliance with the PCI-DSS was a general obligation not owed to plaintiff in particular); *Digital Fed. Credit Union*, 2012 WL 1521479, at *3-4 (finding that breached grocery store owed no duty to issuing bank under Maine law, in part because the parties' risks were allocated in the Card Operating Regulations); cf. *Cumis Ins. Soc'y, Inc. v. Merrick Bank Corp.*, No. CIV 07-374-TUC-CKJ, 2008 WL 4277877, at *11-12 (D. Ariz. Sept. 18, 2008) (dismissing negligence claim asserted by insurer on behalf of issuing credit unions for failure to plead duty under Arizona law).⁴

⁴ Target is aware of only one case in which a court has held that a merchant owed an issuing bank a common-law duty of care. See *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 359 F. Supp. 2d 183, 193-95 (M.D. Pa. 2005). In that case, the negligence claim against the merchant was subsequently dismissed under the economic loss doctrine, 427 F. Supp. 2d 256, 534, and the ruling as to duty was thus never appealed. The decision is, in any event, inapposite for purposes of determining if the Banks have met their burden under Minnesota law, because the *Sovereign Bank* court did not require the plaintiff to plead a special relationship between itself and the defendant in order to survive dismissal. See *id.* Other courts, moreover, have expressly declined to follow the reasoning of the *Sovereign Bank* court. See, e.g., *Digital Fed. Credit Union*, 2012 WL 1521479 at *2-3 (rejecting issuing-bank arguments premised on the *Sovereign Bank* decision after noting that the Supreme Judicial Court of Maine, similar to the Minnesota Supreme Court, was "reticent to recognize new common law duties of care").

Courts similarly have recognized the lack of any duty in negligence between other members of the payment card networks. See *Willingham v. Global Payments, Inc.*, No. 1:12-CV-01157-RWS, 2013 WL 440702, at *18 (N.D. Ga. Feb. 5, 2013) (recommending dismissal where there was "no direct relationship" between cardholders and payment-card processor, and thus no duty in negligence, under Georgia law); see also *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08 Civ. 6060(RMB)(RLE), 2010 WL 2643307, at *9 (S.D.N.Y. June 25, 2010) (bank owed plaintiffs no duty under New York law relating to lost or stolen tapes containing plaintiffs' information, because plaintiffs' information was provided to the bank only through intermediaries, and, thus, the two had no "direct dealings"). Thus, dismissal of the Banks' claim for lack of duty not only is dictated by Minnesota law, but is consistent with the long line of dismissals in other jurisdictions.

2. *The Banks' Allegations of Breach of Duty Fail to Satisfy Iqbal and Twombly.*

Even if the Banks had alleged a duty of care, their allegations of negligent conduct are so conclusory as to fail to state a claim under *Iqbal* and *Twombly*.

The gravamen of the Banks' claim is that Target negligently failed to comply with "industry standards and requirements" – namely, the Card Operating Regulations and the PCI-DSS (Compl. ¶¶ 17–18, 22, 102, 106–07) – but that contention is contradicted by the allegations in the Complaint.⁵

⁵ To the extent the Banks intended their negligence claim to be based in part on Target's alleged failure to comply with the PCSA, the Banks similarly have failed to plead any underlying violation. See *infra*, at Part IV.C.

The Banks allege that the Card Operating Regulations prohibit Target from “disclosing” payment card data, but it is undisputed that the Banks’ claimed injuries resulted not from any disclosure by Target, but from a criminal intrusion in which data was stolen. *See, e.g.,* Compl. ¶¶ 14, 18.

With regard to the PCI-DSS, the Banks do not dispute that just two months before the Intrusion, an independent auditor certified that Target was compliant with “all payment industry requirements, including the [PCI-DSS].” Compl. ¶ 44. While the Banks allege various steps that Target might have taken to “foil” the “hacker’s plan” (*see generally* Compl. ¶¶ 24–59), the Banks claim that just two of Target’s alleged failures to act constituted PCI-DSS violations.⁶ Specifically, the Banks allege that Target “could have” (1) “eliminate[d] unneeded default accounts” and (2) “required vendors to more closely monitor the integrity of their critical file systems” as ostensibly “called for in the PCI-DSS 2.0.” Compl. ¶ 52. However, neither purported PCI-DSS “requirement” actually appears in the laundry list of PCI-DSS requirements recited in the Complaint.

⁶ For example, the Banks make numerous allegations that Target did not act on FireEye malware alerts in time to prevent the intrusion, but do not – and could not – allege that Target’s FireEye-related actions violated the PCI-DSS. *See* Compl. ¶¶ 50–54. Moreover, as the Minnesota Supreme Court has recognized, allowing plaintiffs to proceed on allegations that “further security measures were required” because “existing security precautions [] failed” would provide defendants with “little idea [of] what is expected of him or her” and “discourage [defendants] from improving security.” *Funchess*, 632 N.W.2d at 673 n.4, 675 (emphasis original). Indeed, the Banks admit that FireEye is a “state of art” malware detection tool used by the highest levels of the U.S. security infrastructure, that Target acquired it at a substantial cost in order to address increased cyber-attacks using new and sophisticated techniques, and that Target’s rollout of the tool did not begin until June 2013. Compl. ¶¶ 29, 33–36. To penalize Target for alleged mistakes with respect to FireEye would impose precisely the perverse incentives *Funchess* sought to foreclose.

See Compl. ¶19 (alleging only that use of default *passwords* is prohibited and not referencing vendor security requirements). Further, the only network account referenced in the Complaint is the “limited network credentials” provided to Target’s HVAC vendor (Compl. ¶ 38), which nowhere is alleged to be either unneeded or default. In short, the Banks have utterly failed to allege a violation of the industry standards for data security (i.e., the PCI-DSS) that Target supposedly had a common-law duty to satisfy. For this reason as well, then, their negligence count fails as a matter of law.

B. The Banks’ Claim For Negligent Misrepresentation by Omission Must Also Be Dismissed.

The Complaint asserts as Count IV a claim for negligent misrepresentation by omission. To state a claim for negligent misrepresentation under Minnesota law, a plaintiff must plead that (1) defendant owed plaintiff a duty of care; (2) defendant supplied false information to plaintiff by either including therein a false affirmative representation or omitting therefrom information that renders the facts that are disclosed misleading; (3) plaintiff justifiably and detrimentally relied on the false information from the defendant; and (4) defendant failed to exercise reasonable care in communicating that information. *Noble Sys. Corp. v. Alorica Cent., LLC*, 543 F.3d 978, 985 (8th Cir. 2008); *Kichler v. Wells Fargo Bank, N.A.*, No. 12-1206 (JRT/AJB), 2013 WL 4050204, at *3 (D. Minn. Aug. 9, 2013) (citing *Williams v. Smith*, 820 N.W.2d 807, 815 (Minn. 2012)). Failure to plead any of these elements requires dismissal. *See, e.g., Noble Sys. Corp.*, 543 F.3d at 984–86.

The Banks base their claim on Target's purported misleading omissions in (i) an unspecified "Privacy Policy," (ii) Target's alleged contract with an acquiring bank, in which Target purportedly agreed to comply with the Card Operating Regulations, (iii) an unspecified agreement in which Target allegedly agreed to comply with the PCI-DSS, and (iv) allegedly failing to communicate about the Intrusion in a timely manner. Compl. ¶¶ 18, 128-133. The Banks fail, however, to plead that Target owed them any duty of care in regard to these matters, that Target made any actionable misrepresentation by omission, or that the Banks actually relied upon any of the allegedly false information in question.

1. *The Banks Fail to Allege that Target Owed Them a Duty of Care.*

In the negligent misrepresentation context, "courts distinguish 'between a person engaged in the business or profession of supplying guidance to others and those engaged in commercial transactions at arm's length'" when determining if a defendant owed a plaintiff a duty. *Huntington Bancshares, Inc. v. Ally Fin., Inc.*, No. 27-CV-11-20276, 2012 WL 7749245, ¶ 39 (Minn. Dist. Ct. Dec. 11, 2012) (quoting *Safeco Ins. Co. of Am. v. Dain Bosworth, Inc.*, 531 N.W.2d 867, 871 (Minn. Ct. App. 1995)) (emphasis added). Unless a defendant is in the business of providing guidance to the plaintiff (e.g., an accountant-client, attorney-client, or guardian-ward relationship) – which, like in the negligence context, is referred to as a "special relationship," even though the tests are distinct – no duty is owed. See *Mack*, 2013 U.S. Dist. LEXIS 110142, at *18-22 (granting motion to dismiss for failure to plead duty because there was no special relationship between plaintiff and defendant artist and art dealers arising from sale of

paintings later discovered to be forgeries); *Woodcraft Indus., Inc. v. JBA Int'l, Inc.*, No. 01-373 DWF/RLE, 2001 WL 1640085, at *6 (D. Minn. June 14, 2001) (granting motion to dismiss for failure to plead duty where plaintiff alleged that it and defendant were businesses engaged in a transaction).

The Banks allege that Target is a retailer, not an adviser or fiduciary that is in the business or profession of guiding the Banks in their business transactions. Compl. ¶ 14. Further, Plaintiffs acknowledge that the parties are sophisticated business entities that interact with each other only indirectly (Compl. ¶¶ 7-12, 17-18), which occurs through the separate contracts that the Banks have with the Card Brands, that Target has with its acquiring bank, and that Target's acquiring bank in turn has with the Card Brands. See *supra*, at note 1. Indeed, since the Banks conceded they are not parties to the alleged contract upon which they base much of their claim, in this case Target and the Banks had no commercial relationship whatever, much less a "special" one. And even if they did, that relationship would not differ one iota from the type of arm's length commercial relationship that Minnesota courts have routinely found *insufficient* for purposes of pleading duty in negligent misrepresentation cases. See *Huntington Bancshares*, 2012 WL 7749245, ¶¶ 40-41 (granting motion to dismiss for failure to plead duty where plaintiff alleged it was a consumer bank engaged in mortgage transactions with defendant financial institutions); see also *Regions Treatment Ctr., LLC v. New Stream Real Estate, LLC*, No. 13-1752 ADM/LIB, 2014 WL 107792, slip op. at *7 (D. Minn. Jan. 10, 2014) (denying motion for leave to amend complaint to add claim for negligent misrepresentation because plaintiff was a sophisticated business entity unable to plead

duty); *Woodcraft Indus., Inc.*, 2001 WL 1640085, at *6 (granting motion to dismiss on same grounds).

Even where a party is retained in a fiduciary or professional capacity to provide guidance with respect to a business transaction – which, again, the Banks fall well short of alleging – the resulting duty of care is owed only to those whom the information was intended to guide. *See Noble Sys. Corp.*, 543 F.3d at 985–86. Minnesota courts consistently have denied attempts to extend the duty to plaintiffs who were not parties to the contract at issue, or who were not retained by plaintiffs to provide such guidance. *See id.* (affirming grant of motion to dismiss where plaintiff was not a party to the contract at issue). For example, in *Safeco*, the Minnesota Court of Appeals held that even though the defendant-underwriter was in the business of supplying information for the guidance of its clients, the plaintiff-insurer was *not* defendant’s client for purposes of the bond transaction at issue, and, thus, no duty of care was owed. *See Safeco*, 531 N.W.2d at 872; *see also Adams v. Rosensteel*, No. A13-0451, 2013 WL 6223562, at *3–5 (Minn. Ct. App. Dec. 2, 2013) (affirming grant of motion to dismiss because real estate broker owed a fiduciary duty only to his principal, the seller of a property, and not to plaintiff-buyers).

Here, the Banks’ claim is premised on (i) an unspecified “Privacy Policy” (Compl. ¶ 128), which is not alleged to have been directed to the Banks specifically or even financial intuitions generally, (ii) an agreement between Target and its acquiring bank (Compl. ¶¶ 18, 129), which the Banks do not allege to have ever even seen, much less to have been the intended beneficiaries of, (iii) an unspecified agreement in which Target allegedly agreed to comply with the PCI-DSS, which again the Banks do not claim to

have been a party to or an intended third-party beneficiary of, and (iv) Target’s alleged failure to timely communicate information to unspecified persons or entities concerning the Intrusion (Compl. ¶ 134). Because the Banks have not alleged that they were the intended recipient of any of the allegedly false information in question, they would have failed to plead that Target owed *them* a duty of care in generating that information even if they had a plausible basis to allege that Target generated that information in the capacity of a business providing guidance to *someone else* (as noted above, no such basis exists).

Dismissal of the Banks’ negligent misrepresentation claim for failure to plead duty is also consistent with decisions reached in other data breach cases involving similar allegations. In *Cumis Insurance Society*, 2008 WL 4277877, for example, the court dismissed claims based on alleged misrepresentations about defendants’ compliance with the Card Operating Regulations, because the plaintiff insurance company did not allege that the defendant made any representations to plaintiff or its insureds (issuing banks) distinct from representations made to all participants in the Visa and MasterCard payment systems. *Id.* at *11–12.

In cases premised on a defendant’s alleged failure to promptly inform third parties of an intrusion, courts have routinely found that no legal duties or remedies exist beyond those imposed by statute. *See In re Hamaford Bros. Co. Customer Data Sec. Breach Litig.*, 613 F. Supp. 2d 108, 124–25 (D. Me. 2009) (dismissing negligent misrepresentation by omission claim based on defendants’ alleged failure to notify plaintiffs of an intrusion where the state’s “detailed” data breach notification statute left the court “wary of creating any new state standards where the Maine Law Court has not

already clearly provided a remedy”), *aff’d in part and rev’d in part sub nom Anderson v. Hamnford Bros. Co.*, 659 F.3d 151 (1st Cir. 2011); *see also Willingham*, 2013 WL 440702, at *18 (recommending dismissal where state statute did not require defendant to notify plaintiffs). In Minnesota, the data breach notification law does not require any notification to issuing banks. *See* Minn. Stat. § 325E.61(a) (2013). Thus, the Banks’ allegations seek not only the creation of a new common-law duty, but one that subverts the clear limitations imposed by the Minnesota Legislature.

2. *The Banks Fail to Allege Any Actionable Misrepresentation by Omission.*

The Banks also fail to allege any actionable misrepresentation by omission. It is well-established that claims for negligent misrepresentation and omission are subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b). *See, e.g., Trooten v. Mansour*, 608 F.3d 1020, 1028 (8th Cir. 2010) (negligent misrepresentation is “an allegation of fraud which must be pled with particularity”). Rule 9(b) requires a plaintiff to state claims with particularity, and to accompany such claims with “the who, what, where, when, and how” of the alleged deception. *Sneh v. Bank of N.Y. Mellon*, Civ. No. 12 -954 (MJD/JSM), 2012 WL 5519690, at *7 (D. Minn. Oct. 30, 2012), *adopted by* 2012 WL 5519682 (D. Minn. Nov. 14, 2012) (quoting *BJC Health Sys. v. Columbia Gas. Co.*, 478 F.3d 908, 917 (8th Cir. 2007)); *see also Cox v. Mortg. Elec. Registration Sys.*, 685 F.3d 663, 673 (8th Cir. 2012) (holding that plaintiffs “must plead the time, place, and contents of” false representations, as well as the identity of the party making them), *In re Digi Int’l Inc. Sec. Litig.*, 6 F. Supp. 2d 1089, 1104 (D. Minn. 1998).

The Complaint points to two sets of purportedly deceptive representations regarding Target’s information security, neither of which is adequately pled. First, the Banks cite an unspecified “Privacy Policy” and “other actions and representations” in which Target allegedly “held itself out to the Banks and the FI Class” as having security measures “sufficient to protect” shoppers’ information. Compl. ¶ 128. But the Complaint fails to provide even basic facts about the “Privacy Policy”: when it was issued, the statements made therein through which Target allegedly “held itself out” to the Banks, the specific information Target purportedly omitted, or how any such statements were directed to the Banks for guidance in their business transactions. The Complaint similarly provides no detail whatsoever regarding the alleged “other actions and representations.” Conclusory allegations such as these fail to meet even Rule 8 pleading standards, much less the heightened requirements of Rule 9(b). *Cf. Riley v. Cordis Corp.*, 625 F. Supp. 2d 769, 786–87 (D. Minn. 2009) (granting motion to dismiss even though plaintiff “described[] the contents, as well as the time and place” of some alleged misrepresentations but did “not allege[], with specificity, who made the representations, when the representations were made, [or] to whom the representations were made”).

Second, the Banks allege that Target “agree[d] to comply with both Card Operating Regulations and the PCI-DSS” when it purportedly “knew or should have known that it was not in compliance” with them. Compl. ¶¶ 129–30. The Complaint, again, fails to set forth basic facts about the purported representations, such as the identity of the acquiring bank(s) or other third party with which Target purportedly

CASE 0:14-md-02522-PAM Document 185 Filed 09/02/14 Page 25 of 34

contracted, when the alleged agreement(s) were executed, the terms of any such agreements, the specific information allegedly omitted, and when and how the agreements' terms were directed to the Banks. See Compl. ¶¶ 18, 129–30. Moreover, the Banks fail to plead any violation of either the Card Operating Regulations or the PCI-DSS, much less with the particularity required by Rule 9(b). See *supra*, at Part IV.A.2.

Even if the Banks had satisfied Rule 9(b), their negligent misrepresentation claim would still fail to allege an actionable misrepresentation. In dismissing claims for negligent misrepresentation, this Court previously has recognized that “it is not possible to be negligent in failing to ascertain the truth or falsity of one’s present intention to act in the future.” See *Mitchell v. Franklin Bank, S.S.B.*, No. Civ. 05-1320 PAMRLE, 2005 WL 2406034, at *3 (D. Minn. Sept. 29, 2005) (dismissing claim premised on defendant’s purported negligent misrepresentations about its intent to comply with federal law and pay operating expenses). Thus, any assertion that Target negligently represented its intent to maintain security measures “sufficient to protect” shoppers’ information or to comply with Card Operating Regulations or the PCI-DSS fails as a matter of law. See Compl. ¶ 128. Minnesota courts, moreover, consistently have found that negligent misrepresentation claims premised on contractual provisions are not actionable, holding that to allow otherwise would contravene the law of contracts. See *e.g.*, *Safeco*, 531 N.W.2d at 871; *Woodcraft Indus., Inc.*, 2001 WL 1640085, at *6.

Notably, courts in other data breach cases have explicitly rejected the very argument that the Banks assert here. See *e.g.*, *In re Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566, 594–96 (S.D. Tex. 2011)

23

CASE 0:14-md-02522-PAM Document 185 Filed 09/02/14 Page 26 of 34

(granting motion to dismiss issuing banks’ claim that a payment processor negligently misrepresented its compliance with the Card Operating Regulations, because the Regulations themselves “provide compensation if circumstances later prove that representation false” and because plaintiffs did not allege that defendant never intended to comply with them), *rev’d on other grounds*, 729 F.3d 421 (5th Cir. 2013); *Cumis Ins. Soc’y, Inc. v. B/I’s Wholesale Club*, 918 N.E.2d 36, 49 (Mass. 2009) (affirming summary judgment for breached retailer on negligent misrepresentation claim because “failure to perform a contractual duty [to comply with the Card Operating Regulations] does not give rise to a tort claim for negligent misrepresentation” and because there was no evidence that defendants did not intend to comply with Card Operating Regulations when they entered the contract).

As to the Banks’ allegation that Target “failed to timely communicate information concerning the data breach” (Compl. ¶ 133), that assertion on its face cannot be the basis for a negligent misrepresentation claim, for it concerns only the timeliness of Target’s communications, and not whether the content of any such communication was false. See *Kichler*, 2013 WL 4050204, at *3 (negligent misrepresentation requires false information through either “an affirmative statement that is itself false or” “concealing or not disclosing certain facts that render the facts that are disclosed misleading.”). Moreover, the assertion simply is not plausible, given that Target’s notice was provided within four

24

days of confirming the intrusion.⁷ See Compl. ¶68 n.2. Thus, no actionable misrepresentation by omission is alleged in that regard either.

3. *The Banks Have Failed to Allege Reliance.*

Even if the Banks had alleged a duty and an actionable misrepresentation by omission, Count IV is nonetheless defective because the Banks fail to allege reliance.

In order to state a negligent misrepresentation claim under Minnesota law, a plaintiff must allege that it actually read and relied upon the misrepresentations or omissions alleged, setting forth specifically how and why their reliance caused them harm. See *In re Digi.*, 6 F. Supp. 2d at 1104 (granting motion to dismiss where plaintiff alleged only that it “directly or constructively relied on” the alleged statements and omissions at issue). These allegations must be pled with particularity under Rule 9(b); conclusory allegations of reliance do not suffice. *Cox*, 685 F.3d at 672–74 (affirming grant of motion to dismiss where plaintiffs failed to allege how reliance on particular representations proximately caused their home foreclosure).

Here, the Complaint is devoid of any allegation as to reliance on any of the alleged misrepresentations, even a conclusory one. No Plaintiff alleges that it read the “Privacy Policy,” the alleged agreement between Target and its acquiring bank, the unspecified agreement in which Target allegedly agreed to comply with the PCI-DSS, or any other

⁷ Minnesota’s data breach notification statute (which, as noted above, does not require notice to the Banks) does not specify an amount of time that constitutes “unreasonable delay.” See Minn. Stat. § 325E.61(a). All of the state data breach notification statutes that do so specify, however, indicate that 4 days is more than reasonable. Fla. Stat. § 817.5681(1)(a) (allowing 45 days following discovery); Ohio Rev. Code § 1349.19(B)(1) (same); Wis. Stat. § 134.98(3)(a) (same); cf. Me. Rev. Stat. tit. 10, § 1348(3) (allowing 7 days after law enforcement approval).

document in which the allegedly false information supposedly generated by Target allegedly may have appeared, and no Plaintiff alleges that it undertook or refrained from undertaking any particular action in detrimental reliance upon the allegedly false information contained within those documents or as a result of Target’s alleged failure to timely communicate information about the intrusion. See, e.g., *Raden v. BAC Home Loans Servicing, LP*, No. 12-CV-1240 (PJS/TNL), 2013 WL 656624, at *4–5 (D. Minn. Feb. 22, 2013) (granting motion to dismiss where plaintiffs did not plead with particularity what “loss-mitigation options” they would have successfully pursued and how, absent reliance on defendant’s misrepresentation); see also *Hearland*, 834 F. Supp. 2d at 594 (finding reliance not adequately pled in data breach case where plaintiffs did not allege “that any representations by the defendants induced them to become or remain issuers in the Visa and MasterCard system, or that they have withdrawn from or altered their participation in the system after becoming aware of the defendants’ breach”) (quoting *Cumis Ins. Soc’y, Inc.*, 918 N.E.2d at 49).

C. *The Banks’ Claim For Violation of the Minnesota Plastic Card Security Act Must Be Dismissed.*

1. *The Banks Fail to Allege that Target Retained Any Payment Card Data in Violation of the Minnesota Plastic Card Security Act.*

The Banks’ own allegations rebut their claim in Count Two that Target violated the PCSA. The PCSA prohibits merchants “conducting business in Minnesota” from retaining three types—and only three types—of payment card data after a transaction has been authorized: (1) card security code data, (2) PIN verification code numbers, and (3)

the full contents of any track of magnetic stripe data.⁸ Minn. Stat. § 325E.64, subd. 2. If a merchant violates the PCSA and the impermissibly stored data is “affected by [a data] breach,” the PCSA provides that the merchant must reimburse issuing banks that issued affected cards for “the costs of reasonable actions undertaken by the financial institution as a result.” *Id.* at subd. 3.

Tracking the text of the statute, the Banks allege that Target violated the PCSA “by retaining the card security code data, the PIN verification code number, and/or the full contents of Target customers’ magnetic stripe data,” and that they “suffered injury” as “a direct and proximate result of Target’s violation.” Compl. ¶¶ 118, 120. The Banks allege nothing whatsoever in support of their conclusory claim that Target stored PIN verification code numbers or full magnetic stripe data post-authorization, much less that any such stored data was affected by the Intrusion. As for card security codes, the *only* “fact” that the Banks allege is that an analyst with no connection to Target speculated that “[t]he fact that three-digit CVV security codes were compromised shows they were being stored.”⁹ Compl. ¶ 82. The Banks’ own allegations, however, highlight the flaw in that

⁸ The Banks allege that the PCSA bars storage of all in-scope data types only if stored for more than 48 hours after authorization. Compl. ¶ 114. The 48-hour provision, in fact, only applies to PIN debit transactions. Minn. Stat. § 325E.64, subd. 2. This distinction, however, is immaterial here because the Banks do not plausibly allege that Target stored any of the three data types for any period of time, much less 48 hours post-authorization. ⁹ The Banks’ other allegations regarding customer data storage do not involve the types of data that the PCSA covers. The Banks’ allegation that Target “improperly retained customer data (potentially for many months)” was based on Target’s announcement that the Intrusion involved “names, mailing address, phone numbers, and email address.” Compl. ¶ 75 (emphasis added). None of these data types is in-scope for the PCSA. Minn. Stat. § 325E.64, subd. 2. The Banks’ allegation that Target stored “full [payment card] account number[s]” along with “the expiration date and the cardholder’s name,” Compl.

analyst’s logic and why their PCSA claim must be dismissed: cyber criminals are fully capable of stealing payment card data that was never stored by a merchant for future use, and that is exactly what occurred here.

As the Banks acknowledge, the criminal intruders’ point-of-sale malware was designed to steal payment card data “*in real time*” – not after the transaction had been authorized – “each time customers swiped their card at a Target store.”¹⁰ Compl. ¶ 56 (emphasis added). As the Complaint describes it, the malware

actively collect[ed] card records from live customer transactions. The way the malware worked was simple: when a customer went to any in-store Target cash register to pay for an item and swiped his or her card, the malware stepped in and captured the shopper’s card number and other sensitive financial information.

Compl. ¶ 49 (emphasis added). The Banks’ description of the Intrusion, moreover, nowhere suggests that the intruders used any mechanism other than the point-of-sale malware described above to capture the allegedly stolen payment card data that underlies all of the Banks’ alleged injuries. See Compl. ¶¶ 47–67. The Banks’ allegation that Visa had previously issued reports “alerting Target to attacks using RAM scraper malware, or

¶ 82, is similarly irrelevant for purposes of determining if Target violated the PCSA because the “full magnetic stripe data” that cannot be stored under the PCSA is composed of name, card number, expiration date and a security code, such as a CVV. Cf. Compl. ¶ 71 (describing the elements of “full magnetic stripe data”). Nowhere, moreover, do the Banks allege that the particular payment card data referenced in Paragraph 82 was affected by the Intrusion.

¹⁰ The Banks allege that after the “real-time” data capture, “the hackers temporarily stored the data” in staging points on Target’s network for six days before exfiltrating it. Compl. ¶ 56 (emphasis added). Even if this were true, it would not salvage the Banks’ PCSA claim, since the PCSA only addresses data storage by a merchant or by a merchant’s service provider. Minn. Stat. § 325E.64, subd. 2.

memory parsing software, which enables cyber criminals to grab encrypted data by *capturing it when it travels through the live memory of a computer.*" Compl. ¶ 30, underscores that the simple fact that payment card data is stolen does not mean that the merchant at issue has been storing it, as the analyst asserted.

The Banks' claim is, therefore, particularly ripe for dismissal since they not only failed to plead facts to support Target's alleged violation of the PCSA, but actually pleaded facts that "would appear to refute any such conclusion." *Clark v. Northland Grp., Inc.*, No. 14-606 (PAM/IJC), 2014 WL 3828218, slip op. at 3 (D. Minn. Aug. 4, 2014); *see also Lubbers v. Deutsche Bank Nat. Trust Co.*, No. 13-926 (DWF/ISM), 2013 WL 6729004, slip op. at 12 (D. Minn. Dec. 19, 2013) (granting motion to dismiss where exhibits to the complaint where "in direct contradiction to plaintiff's factually devoid assertions"). Since the only "fact" supporting the Banks' allegation of a PCSA violation – an analyst's opinion – is undercut by the Banks' own description of how the intrusion occurred, the Banks are left with nothing more than "a formulaic recitation of the elements of a cause of action" that cannot survive a motion to dismiss. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

2. The Minnesota Plastic Card Security Act Only Applies to Business Conducted in Minnesota.

The PCSA only applies when an entity is "conducting business in Minnesota [and] accepts an access device in connection with a transaction." Minn. Stat. § 325E.64, subd. 2. Accordingly, even if the Banks had pled facts sufficient to state a claim under the PCSA – as set forth above, they have not – their PCSA claim should still be dismissed to

the extent it is based on underlying customer transactions that occurred in states other than Minnesota.¹¹

D. Because the Banks Have Failed to State a Claim For Violation of the Minnesota Plastic Card Security Act, They Have Likewise Failed to State a Claim For Negligence Per Se Based on that Act.

In Minnesota, certain statutory violations can substitute for the duty and breach elements of a claim for ordinary negligence, converting it to a negligence *per se* claim. *Mervin v. Magney Constr. Co.*, 399 N.W.2d 579, 582 (Minn. Ct. App. 1987). The Banks in Count Three assert that Target's "violation of the [PCSA] constitutes negligence *per se*." Compl. ¶ 126. As discussed above, however, the Banks have failed to plead a violation of the underlying statute and thus have failed to plead a breach of duty. The negligence *per se* claim therefore necessarily fails. *Yang Mee Thao-Xiong v. Am. Morig. Corp.*, No. 13-CV-354 (MJD/TNL), 2013 WL 3788799, slip op. at 2 (D. Minn. July 18, 2013) (dismissing negligence *per se* claim where the plaintiffs' amended complaint itself confirmed that no underlying statutory violation had occurred).

V. CONCLUSION

For the foregoing reasons, Target respectfully requests that the Court grant Target's motion to dismiss the Complaint in its entirety.

¹¹ Notably, an interpretation of the PCSA as applicable to transactions in stores outside Minnesota with non-Minnesota shoppers would require dismissal of the Banks' entire PCSA claim, since it would impose conditions on "commerce occurring entirely outside the boundaries of" Minnesota and, therefore, violate the "dormant" component of the Commerce Clause of the U.S. Constitution. *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989); *see also Cotto Wazo Co. v. Williams*, 46 F.3d 790, 793 (8th Cir. 1995) ("Extraterritorial reach invalidates a state statute when the statute requires people or businesses to conduct their out-of-state commerce in a certain way.").

Computer Law Reporter

1601 Connecticut Avenue, N.W., Suite 701, Washington, DC 20009 • 202-462-5755 • Fax 202-328-2430

Respectfully submitted,

Date: September 2, 2014

/s/ Wendy J. Wildung

Wendy J. Wildung, #117055

Michael A. Ponto, #203944

FAEGRE BAKER DANIELS LLP

2200 Wells Fargo Center

90 South Seventh Street

Minneapolis, MN 55402-3901

P: (612) 766-7000

F: (612) 766-1600 (Facsimile)

wendy.wildung@faegrebd.com

michael.ponto@faegrebd.com

Douglas H. Meal

ROPES & GRAY LLP

Prudential Tower

800 Boylston Street

Boston, MA 02199-3600

P: (617) 951-7000

F: (617) 951-7050

Douglas.Meal@ropesgray.com

Michelle Visser

ROPES & GRAY LLP

Three Embarcadero Center

San Francisco, CA 94111-4006

P: (415) 315-6300

F: (415) 315-6350

Michelle.Visser@ropesgray.com

Attorneys for Defendant Target Corporation

US 54791500.01

Computer Law Reporter

Recent Decisions Index

TCPA: VICARIOUS LIABILITY; SETTLEMENT OFFERS; FIRST AMENDMENT

Gomez v. Campbell-Ewald Co. No. 13-55486 (9th Cir. Sep. 19, 2014)

Ninth Circuit Refuses Summary Judgment to U.S. Navy’s Advertising
Agency That Allegedly Violated TCPA By Hiring Contractor To Send
Unauthorized Text Recruitment Messages; Settlement Offer
to Plaintiff Did Not Moot Class Action30

CUSTOMER RECORDS ACT; UCL; DATA BREACH; STANDING; RESTITUTION; MOTION TO DISMISS

In re Adobe Systems, Inc. Privacy Litigation, 13–CV–05226–LHK (N.D. Cal., Sep. 4, 2014)

Federal Court Holds That Plaintiffs Had Standing To Sue Under
Article III and California Law Based on the Threat Their
Personal Data Would Be Misused Following a Major Data Breach32

CIPA; CLASS ACTION; RULE 23; SUPERIORITY; PREDOMINANCE; DUE PROCESS; CERTIFICATION

Ades v. Omni Hotels Management Corp., No. 2:13–cv–02468–CAS(MANx) (Doc No. 80)
(C.D. Cal. Sep. 8, 2014)

Federal Court Certifies Class Action Consisting of Members
Whose Phone Calls Were Recorded Without Consent.....36

CIPA; CALL CENTER; CHOICE OF LAW; DORMANT COMMERCE CLAUSE; SUMMARY JUDGMENT

Ades v. Omni Hotels Management Group, No. 2:13–CV–2468–CAS(MANx) (Doc. No. 81) (C.D. Cal. Sep. 8, 2014)

Federal Court Denies Defendants Summary Judgment in CIPA Class
Action and Holds That Application of CIPA Did Not Violate the
Dormant Commerce Clause40

CFAA; AMENDMENT; AUTHORIZED; LOSS; DAMAGES; MOTION TO DISMISS

Jung v. Chorus Music Studio, No. 13–CV–1494 (CM)(RLE) (S.D. N.Y. Sep. 11, 2014)

Federal Court Holds That a CFAA Counterclaim Would Not Be
Futile Even Though the Proposed Counterclaim Did Not Allege
Unauthorized Access44

DATA BREACH; ARTICLE III STANDING; CONCRETE; CREDIT CARD; MOTION TO DISMISS

Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735 (N.D. Ill. Sep. 16, 2014)

Federal Court Holds That Department Store Customers Whose Credit Card
Information Was or May Have Been Stolen Lacked Standing
Because They Had Not Incurred a Concrete Injury46

CONTENT REGULATION

Three D, LLC d/b/a Triple Play Sports Bar and Grille and Jillian Sanzone / Spinella, No.
34-CA-012915 (NLRB, Aug. 22, 2014)

NLRB Invalidates Employer’s Blogging Policy
and Reverses Firing Based On Facebook Posts51

EVIDENCE/DISCOVERY; LICENSING/CONTRACTS

Turner v. Temptu Inc., No. 13-3440 (2d Cir. Sept. 23, 2014)

Jointly Editable Online Document Doesn’t
Provide Evidence of Contract Formation55

CONTENT REGULATION; DERIVATIVE LIABILITY

Jane Doe No. 14 v. Internet Brands, Inc., No. 12-56638 (9th Cir. Sept. 17, 2014)

9th Circuit Creates Problematic “Failure To Warn”
Exception to Section 230 Immunity56

PRIVACY/SECURITY; PUBLICITY/PRIVACY RIGHTS

Sunbelt Rentals v. Victor, No. 13-4240-SBA (N.D. Cal. Aug. 28, 2014)

Employer Isn’t Liable When Former Employee
Linked His Apple Accounts To Its Devices63

PRIVACY/SECURITY

Zaratzian v. Abadir, 10 CV 9049 (VB) (S.D.N.Y. Sept 2, 2014)

When Is It Appropriate To Monitor An Ex-Spouse’s Email Account? Never67

COPYRIGHT; LICENSING/ CONTRACTS

AFP v. Morel, 10-cv-2730 (AJN) (S.D.N.Y. Aug. 13, 2014)

Court Denies AFP/Getty Bid to Set Aside Morel Copyright Verdict.....70

E-COMMERCE; MARKETING

Imber-Gluck v. Google, 14-cv-1070 (N.D. Cal. July 21, 2014)

Lawsuit Against Google Over In-App Purchases
By Minors Squeaks Past Motion to Dismiss.....73

Recent Decisions

TCPA: VICARIOUS LIABILITY; SETTLEMENT OFFERS; FIRST AMENDMENT

Gomez v. Campbell-Ewald Co. No. 13-55486 (9th Cir. Sep. 19, 2014)

Ninth Circuit Refuses Summary Judgment to U.S. Navy’s Advertising Agency That Allegedly Violated TCPA By Hiring Contractor To Send Unauthorized Text Recruitment Messages; Settlement Offer to Plaintiff Did Not Moot Class Action

In a case where the Navy hired an advertising agency to obtain recruitments and the agency hired a contractor to send unsolicited text messages, the Ninth Circuit reversed a District Court ruling that the agency was immune from liability because a defendant may be held vicariously liable for TCPA violations where the plaintiff establishes an agency relationship, as defined by federal common law, between the defendant and a third-party caller.

The court also held that pursuant to *Diaz v. First Am. Home Buyers Prot. Corp.*, 732 F.3d 948 (9th Cir. 2013), the plaintiff’s individual claim was not mooted by his refusal to accept a settlement offer under Federal Rule of Civil Procedure 68. Pursuant to *Pitts v. Terrible Herbst, Inc.*, 653 F.3d 1081 (9th Cir. 2011), the putative class claims were not mooted where the plaintiff rejected the settlement offer before he moved for class certification. The panel concluded that *Pitts* and *Diaz* were not clearly irreconcilable with *Genesis Healthcare Corp. v. Symczyk*, 133 S. Ct. 1523 (2013) (addressing collective action brought pursuant to Fair Labor Standards Act).

The panel further held that 47 U.S.C. § 227(b)(1)(A)(iii), which restricts unsolicited text messaging, does not violate the First Amendment and that the defendant was not entitled to derivative sovereign immunity.

According to the court:

Although Campbell-Ewald did not send any text messages, it might be vicariously liable for the messages sent by Mindmatics. The statute itself is silent as to vicarious liability. We therefore assume that Congress intended to incorporate “ordinary tort-related vicarious liability rules.” *Meyer v. Holley*, 537 U.S. 280, 285 (2003). Accordingly, “[a]bsent a clear expression of Congressional intent to apply another standard, the Court must presume that Congress intended to apply the traditional standards of vicarious liability” *Thomas v. Taco Bell Corp.*, 879 F. Supp. 2d 1079, 1084 (C.D.

Cal. 2012), *aff'd*, — F.App'x —, 2014 WL 2959160 (9th Cir. July 2, 2014) (per curiam). Although we have never expressly reached this question, several of our district courts have already concluded that the TCPA imposes vicarious liability where an agency relationship, as defined by federal common law, is established between the defendant and a third-party caller.

...Given Campbell-Ewald's concession that a merchant can be held liable for outsourced telemarketing, it is unclear why a third-party marketing consultant shouldn't be subject to that same liability. As a matter of policy it seems more important to subject the consultant to the consequences of TCPA infraction. After all, a merchant presumably hires a consultant in part due to its expertise in marketing norms. It makes little sense to hold the merchant vicariously liable for a campaign he entrusts to an advertising professional, unless that professional is equally accountable for any resulting TCPA violation. In fact, Campbell-Ewald identifies no case in which a defendant was exempt from liability due to the outsourced transmission of the prohibited calls...

...Finally, we turn to the legal theory underlying the district court's decision. The court entered summary judgment after concluding that Campbell-Ewald is exempt from liability under *Yearsley*, 309 U.S. 18. Gomez contends that *Yearsley* is outdated and inapposite, and that the district court should have applied the standard articulated in *Boyle v. United Technologies Corp.*, 487 U.S. 500 (1988). The availability of these defenses is a question of law that we review *de novo*. *In re Hanford Nuclear Reservation Litig.*, 534 F.3d 986, 1000 (9th Cir. 2008)...

...Campbell-Ewald contends that a new immunity for service contractors was espoused by the Supreme Court in *Filarsky v. Delia*, — U.S. —, 132 S.Ct. 1657 (2012). Yet the Court did not establish any new theory, and although the *Filarsky* discussion does include a broad reading of the qualified immunity doctrine, *id.* at 1667–68, that doctrine is not implicated by this case. *Filarsky* involved alleged constitutional violations brought pursuant to 42 U.S.C. § 1983. *See id.* at 1661. The Supreme Court granted certiorari to resolve a dispute as to whether one of the defendants—an attorney contracted by municipal government—was eligible for the qualified immunity afforded to his city-employed colleagues. *Id.* at 1660–61. To determine the scope of the doctrine, the Court examined “the ‘general principles of tort immunities and defenses’ applicable at common law.” *Id.* at 1662 (quoting *Imbler v. Pachtman*, 424 U.S. 409, 418 (1976)). When the examination revealed that part-time and lay officials had been granted immunity throughout the nineteenth century, *id.* at 1665, the Court concluded that the contractor was properly entitled to the same qualified immunity enjoyed by his publicly employed counterparts.

* * *

CUSTOMER RECORDS ACT; UCL; DATA BREACH; STANDING; RESTITUTION; MOTION TO DISMISS

In re Adobe Systems, Inc. Privacy Litigation, 13–CV–05226–LHK (N.D. Cal., Sep. 4, 2014)

Federal Court Holds That Plaintiffs Had Standing To Sue Under Article III and California Law Based on the Threat Their Personal Data Would Be Misused Following a Major Data Breach

In this consolidated action, plaintiffs seek injunctive and declaratory relief and restitution on behalf of a class of Adobe customers whose personal information was accessed by hackers during a breach of Adobe’s servers. The Court reaffirmed a Ninth Circuit opinion to the effect that an imminent threat that hacked personal information will be misused is sufficient to provide Article III standing, even if the misuse is not absolutely certain to occur. Contrary to some other district courts, the Court did not read the Supreme Court’s *Clapper* decision as holding that the threat of misuse of hacked data is generally insufficient to confer standing on plaintiffs whose data was taken but has not yet known to have been misused. The Court also held that a state law restitution claim could be brought here even though the named plaintiffs did not subscribe to all the Adobe services that are encompassed within the proposed class definition. With respect to most of the named plaintiffs, the Court denied the motion to dismiss in its entirety.

Background

Adobe is a multinational software company that sells and licenses printing, publishing, multimedia, and graphics software. In July 2013, hackers gained unauthorized access to Adobe’s servers. The data breach did not come to light until September, when independent security researchers discovered stolen Adobe source code on the Internet. Adobe announced that the hackers accessed the personal information of at least 38 million customers, including names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses. Following the 2013 data breach, researchers concluded that Adobe’s security practices were deeply flawed and did not conform to industry standards. Plaintiffs are customers of Adobe licensed products or Creative Cloud subscribers who provided Adobe with their personal information.

Standing for Customer Records Act Claim

Plaintiffs’ first cause of action was for injunctive relief on behalf of the California Plaintiffs for violations of Sections 1798.81.5 and 1798.82 of the California Civil Code (CRA). Adobe argued that plaintiffs do not allege injury-in-fact resulting from Adobe’s

alleged violation of the CRA and thus do not have Article III standing to bring their CRA claim. Plaintiffs claimed that they are all at increased risk of future harm as a result of the 2013 data breach. Adobe countered that such “increased risk” is not a cognizable injury for Article III standing purposes. The Ninth Circuit addressed Article III standing in the context of stolen personal information in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir.2010). In *Krottner*, a thief stole a laptop from Starbucks containing the unencrypted names, addresses, and social security numbers of roughly 97,000 Starbucks employees. *Id.* at 1140. The Ninth Circuit disagreed, holding instead that “the possibility of future injury may be sufficient to confer standing” where the plaintiff is “*immediately* in danger of sustaining some *direct* injury as the result of the challenged conduct.” Adobe did not dispute that *Krottner* is directly on point. However, Adobe contended that subsequent Supreme Court authority forecloses the approach the Ninth Circuit took to standing in *Krottner*. Specifically, Adobe claimed that the Supreme Court’s decision in *Clapper v. Amnesty International USA* expressly held that “[a]llegations of *possible* future injury” cannot be a basis for Article III standing, and instead required instead that a “threatened injury [] be *certainly impending* to constitute injury in fact.” Adobe argued that following *Clapper* district courts in data breach cases regularly conclude that increased risk of future harm is insufficient to confer Article III standing under the “certainly impending” standard. Adobe encouraged this Court to conclude that *Clapper* implicitly overruled *Krottner*.

As the Supreme Court noted, the respondents in *Clapper* did not allege that any of their communications had actually been intercepted, or even that the Government sought to target them directly. The Supreme Court acknowledged that its precedents “do not uniformly require plaintiffs to demonstrate that it is *literally certain* that the harms they identify will come about” in order to have standing. Rather, in some cases, the Supreme Court has found standing “based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm.”

Clapper did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact, causation, and redressability. The Court thus did “not find that *Krottner* and *Clapper* are clearly irreconcilable.” “*Krottner* did use somewhat different phrases to describe the degree of imminence a plaintiff must allege in order to have standing based on a threat of injury,” but “this difference in wording is not substantial.” “Given that *Krottner* described the imminence standard in terms similar to those used in *Clapper*, and in light of the fact that nothing in *Clapper* reveals an intent to alter established standing principles, the Court cannot conclude that *Krottner* has been effectively overruled.”

In any event, even if *Krottner* were no longer good law, “the threatened harm alleged here is sufficiently concrete and imminent to satisfy *Clapper*.” Unlike in *Clapper*, where respondents’ claimed that they would suffer future harm rested on a chain of events that was both “highly attenuated” and “highly speculative,” the risk “that Plaintiffs’ personal data will be misused by the hackers who breached Adobe’s network is immediate and very real.” Plaintiffs alleged that the hackers deliberately targeted Adobe’s servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. “In sum, the Court finds that Plaintiffs’ allegations of a concrete and imminent threat of future harm suffice to establish Article III injury-in-fact at the pleadings stage under both *Krottner* and *Clapper*.”

“As Adobe does not contend, and as the Court has no reason to believe, that the CRA’s statutory standing requirements are more stringent than Article III’s, the Court finds that Plaintiffs’ allegations of injury-in-fact satisfy the CRA’s statutory standing requirement for the same reasons these allegations satisfy Article III.”

Declaratory Relief

Adobe sought dismissal of plaintiffs’ declaratory relief claim on the ground that plaintiffs do not fulfill the Declaratory Judgment Act’s statutory jurisdictional requirements. Adobe contended that there is no actionable dispute over whether Adobe is in breach of its contractual obligation to provide “reasonable . . . security controls,” given that the Agreement expressly provided that no security measure is “100%” effective and that “Adobe cannot ensure or warrant the security of your personal information.”

The Court found that plaintiffs have adequately alleged the existence of an actionable dispute for purposes of the Declaratory Judgment Act. Plaintiffs have plausibly alleged the existence of a “definite and concrete” dispute over the meaning and the scope of Adobe’s contractual obligation to provide “reasonable” security measures. According to the Complaint, although “Adobe maintains that its security measures were adequate and remain adequate,” there were in fact a number of standard industry practices that Adobe failed to follow. Although Adobe contended that there can be no actionable dispute concerning the adequacy of Adobe’s security controls because the Agreement expressly provides that no security measure is “100%” effective, “this disclaimer does not relieve Adobe of the responsibility (also contained in the Agreement) to provide ‘reasonable’ security, *see* Agreement at 4; Compl. ¶ 120.”

The Court thus concluded “that Plaintiffs have plausibly alleged that they satisfy the statutory jurisdictional requirements for obtaining declaratory relief. Adobe is not entitled to dismissal of Plaintiffs’ claim on this basis.”

UCL Restitution Claim

“Plaintiffs’ fourth and final cause of action is for restitution under the Unfair Competition Law (UCL) on behalf of purchasers of Adobe’s ColdFusion and Creative Cloud products and services.” Plaintiffs asserted claims under both the “fraudulent” and “unfair” prongs of the UCL on the basis that Adobe “fail[ed] to disclose that it does not enlist industry standard security practices.”

Some courts reserve the question of whether plaintiffs may assert claims based on products they did not buy until ruling on a motion for class certification. Others “hold that a plaintiff may have standing to assert claims for unnamed class members based on products he or she did not purchase so long as the products and alleged misrepresentations are substantially similar.” “This Court has previously applied the “substantially similar” approach and will do so again here.” Under this approach, both the products themselves and the misrepresentations the plaintiff challenges must be similar, though not identical. “In this case, the misrepresentations and omissions at issue are the same for both ColdFusion and Creative Cloud, as all Adobe products are governed by the same privacy policy.”

Adobe contended, however, that ColdFusion and Creative Cloud are sufficiently dissimilar *as products* that plaintiffs lack standing to assert claims as to ColdFusion. But the Court found that the differences between ColdFusion and Creative Cloud were not significant enough to prevent the products from being “substantially similar” for purposes of the claims alleged here.

Adobe also argued for dismissal of the UCL claim on the ground that Adobe’s lax security practices were well-known so that there was no material omission or material misrepresentation regarding security practices. The Court was “not convinced.” “It is one thing to have a poor reputation for security in general, but that does not mean that Adobe’s specific security shortcomings were widely known.” None of the press reports Adobe identifies discussed any specific security deficiencies, and plaintiffs expressly alleged that the extent of Adobe’s security shortcomings were revealed only *after* the 2013 data breach.

Given that prior reports of Adobe’s security problems were highly generic, the Court cannot say that Adobe did not have exclusive knowledge of its failure to implement industry-standard security measures. Furthermore, the exact nature of what was in the public domain regarding Adobe’s security practices is a question of fact not properly resolved on a motion to dismiss.

Adobe also argued “that even if Plaintiffs identify an actionable omission, Plaintiffs cannot allege that they relied on that omission, as is required for a claim under the ‘fraudulent’ prong of the UCL.” The Court disagreed. Plaintiffs alleged that they would not have subscribed to Creative Cloud in the first instance had they known of Adobe’s allegedly

unsound security practices. Having invested time, money, and energy in Creative Cloud, plaintiffs alleged that the costs to switch to another product “are now too high to justify abandoning their Creative Cloud subscriptions.”

This is a plausible allegation. Moreover, a plaintiff need not allege that a product became totally worthless to her once the defendant’s misrepresentation came to light in order to plead actionable reliance.

Rather, it is enough to allege that the product is worth *less* to the plaintiff in light of the misrepresentation.

Accordingly, the Court found “that Plaintiffs have not pleaded themselves out of court by alleging that they did not cancel their Creative Cloud subscriptions upon learning of Adobe’s omissions regarding security.”

* * *

CIPA; CLASS ACTION; RULE 23; SUPERIORITY; PREDOMINANCE; DUE PROCESS; CERTIFICATION

Ades v. Omni Hotels Management Corp., No. 2:13–cv–02468–CAS(MANx) (Doc No. 80) (C.D. Cal. Sep. 8, 2014)

**Federal Court Certifies Class Action Consisting of Members Whose
Phone Calls Were Recorded Without Consent**

In this case involving callers to a toll-free phone number whose calls allegedly were recorded without their consent, the Court granted the motion for class certification, holding that the class was reasonably ascertainable and the requirements of Federal Rule 23 had been met. The Court explained that a class action was superior to individual suits because it was unclear that the statutory damages available under the California Invasion of Privacy Act would incentivize individual actions. The Court also suggested that the possibility that an aggregate damages award for the class would be massive and raise Due Process/proportionality concerns was not a proper consideration at the class certification stage and should not preclude certification, particularly given that the California legislature had expressly adopted and retained \$5,000 as the minimum statutory damages for each violation of CIPA.

Background

Plaintiffs contended that they called Omni’s toll-free phone number and, without being warned that their calls were being recorded, provided Omni representatives with personal information including their names, phone numbers, e-mail addresses, and credit card numbers and expiration dates. Plaintiffs alleged that unwarned and unconsented recording and monitoring of inbound calls pursuant to Omni company policy violated § 632.7 of the

California Invasion of Privacy Act or CIPA, entitling them to statutory damages. Plaintiffs sought to certify a class of all individuals who, between March 15, 2012 and March 22, 2013, inclusive (the “Class Period”), while physically present in California, participated in a telephone call with a live representative of Omni that was: (1) placed to [one of several Omni toll-free numbers], (2) made from a telephone number that includes a California area code; and (3) transmitted via cellular telephone on the network of AT & T, Verizon Wireless, or Sprint.

Whether the Class Is Ascertainable

Omni argued that even if the requirements of Rule 23 were met, certification was not appropriate because the classes were not ascertainable. Plaintiffs argued that the proposed class definition sets forth objective criteria by which individuals can identify themselves as members of the class and the court can administratively determine who is a class member. They argued that the Omni Aspect list and telecommunications databases can be used to identify phone calls to Omni during the Class Period associated with California cellular telephone numbers, and that reverse lookup directories or wireless carrier records can be used to identify callers on the Verizon Wireless, AT & T Wireless, and Sprint cellular networks. Plaintiffs contended that the physical location of the caller at the time of the call can be determined objectively through records of the wireless carrier that handled each call, and that reservation records can also help identify class members. Finally, plaintiffs asserted that any difficulties in identifying class members are attributable to Omni’s destruction of data that could have been used to search the audio recordings, and that it would be unfair to allow such difficulties to prejudice class certification.

The Court “does not find a lack of ascertainability to defeat class certification here.” It was “enough that the class definition describes a set of common characteristics sufficient to allow a prospective plaintiff to identify himself or herself as having a right to recover based on the description.” *McCrary v. The Elations Co., LLC*, No. EDCV 13–00242 JGB (OPx), 2014 WL 1779243, at *8 (C.D.Cal. Jan. 13, 2014). Plaintiffs’ class definition set forth objective characteristics sufficient to enable prospective class members to identify themselves. The definition limited the class to those who made a call within a certain time period, while located in a specific geographic area, from a cellular phone, on one of three wireless networks, to a particular set of toll-free telephone numbers. Potential class members can show that they fit the class definition through records identified by plaintiffs showing that the putative class members’ qualifying cellular telephones were used to call one of the specified Omni lines from California during the Class Period.

Predominance

In support of commonality and predominance, plaintiffs asserted that common questions included

(1) whether Omni had a policy and practice of recording calls to the Contact Center; (2) whether Omni had a policy and practice of advising callers that telephone calls are recorded; (3) whether the callers consented to the recording; and (4) the monetary and injunctive remedies to which class members are entitled.

Mem. Supp. Class Cert. at 20–21. Plaintiffs argued that classwide evidence can establish a *prima facie* case that the calls were recorded, that class members were not warned of recording, and that class members did not consent to the recording.

Omni asserted that two types of individual issues would predominate. First, Omni argued that plaintiffs could not prove on a classwide basis the “injury” required to bring a damages action under § 637.2 because some putative class members assumed their calls would be recorded, and therefore suffered no harm from being recorded without warning. But the only “harm” required by § 637.2 “is the unauthorized recording.”

Next, Omni contended that the question of implied consent to recording would require individualized inquiries. Plaintiffs criticized Omni’s conceptualization of and evidence of implied consent. Plaintiffs argued that Omni had not shown that any request to access prior recordings was made by a class member, and that in any event such a request would not show consent.

Omni argued that individual issues of consent would predominate even in the absence of any prior notice, because consent “is an intensely factual question” that “requires looking at all of the circumstances ... to determine whether an individual knew that her communications were being intercepted.” *In re Google, Inc. Gmail Litig.*, No. 13–MD–02430, 2014 WL 1102660, at *16 (N.D.Cal. Mar. 18, 2014).

But Omni cited no case in which a class was rejected on consent grounds despite the absence of any evidence of advance notice. “Despite extensive discovery, Omni has not produced evidence that a single person meeting the class definition actually consented to a call being recorded during the Class Period.” “Thus, unlike in the cases Omni cites, there is no indication that individual consent issues will overwhelm issues plaintiffs have shown to be resolvable through classwide proof.” Therefore, on the record before it, the Court found that plaintiffs had met their burden of showing that common questions would predominate at trial.

Superiority

Plaintiffs submitted that a class action is superior because the only alternative would be “thousands of separate cases litigated from start to finish.” Mem. Supp. Class Cert. at 24. Moreover, they asserted that available damages are insufficient to incentivize individual litigation. Omni responded that adequate incentives exist for individual lawsuits in the form of CIPA’s minimum damages of \$5,000.

Moreover, Omni argued that, when aggregated on a classwide basis, CIPA’s damages would be grossly excessive as to violate the Due Process Clause. Plaintiffs responded that under *Bateman*, consideration of “excessive” statutory damages is improper at the class certification stage.

The Ninth Circuit in *Bateman*

“reserve[d] judgment . . . on whether Rule 23(b)(3) *per se* prohibits consideration of a defendant’s potential liability in deciding whether to certify a class.” Nevertheless, the Court finds sufficient similarities between *Bateman* and this case to decline to consider allegedly excessive damages as weighing against superiority. *Bateman* involved a putative class action brought under the Fair and Accurate Credit Transactions Act (FACTA), a federal statute that, like CIPA, provides for statutory damages upon proof of a privacy violation, without evidence of actual damages.

The Ninth Circuit noted that Congress, despite being aware of the availability of the class action form, did not cap or otherwise limit damages that could be obtained in class actions, as it had for other statutes. The Ninth Circuit reasoned Congress had decided that the penalties it set served compensatory and deterrence functions and were proportionate to the prohibited conduct. “Accordingly, the unanimous panel held that the district court had abused its discretion” by “considering the proportionality of the potential liability to the actual harm alleged in its Rule 23(b)(3) superiority analysis.”

Here, the California Legislature evidently decided that minimum damages of \$5,000 per violation serve CIPA’s purposes and are proportional to the harm caused by CIPA violations. Plaintiffs’ action is not the first class action to be filed under § 637.2, and the Legislature could have acted to limit damages in response to any concerns about the liability sought in previous class actions. “Moreover, for reasons more fully explained in the order denying Omni’s motion for summary judgment, issues of excessive damages are better addressed at a later stage of the litigation.” Finally, “the Court is not persuaded that \$5,000 in damages is so clearly sufficient to motivate individual litigation involving complex factual and legal issues as to weigh against class certification.” Therefore, the Court found that plaintiffs have satisfied their burden of showing superiority.

* * *

CIPA; CALL CENTER; CHOICE OF LAW; DORMANT COMMERCE CLAUSE; SUMMARY JUDGMENT

Ades v. Omni Hotels Management Group, No. 2:13–CV–2468–CAS(MANx) (Doc. No. 81) (C.D. Cal. Sep. 8, 2014)

Federal Court Denies Defendants Summary Judgment in CIPA Class Action and Holds That Application of CIPA Did Not Violate the Dormant Commerce Clause

In this class action lawsuit seeking statutory damages under the California Invasion of Privacy Act (CIPA) based on the alleged recording of customer calls without consent, the Court denied the defendants’ motion for summary judgment. The Court held that California law applied even though the call center was located in Nebraska. The Court also held that application of CIPA to calls made by Californians to the call center in Nebraska did not violate the Dormant Commerce Clause. The Court explained that there was a triable issue as to whether the call center could identify the state of origin of callers, and hence could treat calls from California differently from calls from other states. The Court also suggested that even if CIPA incentivized national call centers to comply with CIPA with respect to *all* incoming calls, CIPA did not necessarily violate the Dormant Commerce Clause. Indeed, CIPA did not in any way represent extraterritorial regulation. The Court also found no merit in defendants’ other arguments for summary judgment.

Background

Plaintiffs brought this suit on behalf of themselves and “[a]ll individuals who, between March 15, 2012 and March 22, 2013, inclusive (the ‘Class Period’), while physically present in California, participated in a telephone call with a live representative of Omni” that was placed to one of several Omni toll-free numbers, made from a telephone number with a California area code, and transmitted via the AT & T, Verizon Wireless, or Sprint cellular telephone networks. Plaintiffs contended that they called Omni’s toll-free phone number and, without being warned that their calls were being recorded, provided Omni representatives with personal information including their names, phone numbers, e-mail addresses, and credit card numbers and expiration dates. Plaintiffs alleged that unwarned and unconsented recording and monitoring of inbound calls pursuant to Omni company policy violated § 632.7 of the California Invasion of Privacy Act or CIPA, entitling them to statutory damages. The calls at issue were placed to an Omni call center located in Omaha, Nebraska. Omni states that all relevant incoming calls were recorded solely for quality assurance purposes. While disputing that this is relevant to the motion for summary judgment, plaintiffs cited evidence that the recordings were also made so that Omni personnel could consult them in the event of a dispute between Omni and a customer.

Choice of Law

Omni argued that “if there is a conflict between California and Nebraska law—that is, if § 632.7 makes illegal non-consensual recordings made for service monitoring purposes—Nebraska’s interests in applying its law outweigh those of California.” Nebraska law permits employers to “intercept, disclose, or use” communications related to “any activity which is a necessary incident to the rendition of ... [its] service or to the protection of the rights or property of the carrier or provider of such communication services.” Neb. Rev.Stat. § 86–920(2)(a). Based on this provision, Omni contended that Nebraska favors allowing businesses to monitor their employees, as to provide better customer service, over protecting consumer privacy directly. Omni argued that the difference in law reflects Nebraska’s attempt to make its state more business-friendly. Moreover, Omni argued that Nebraska law applies because the alleged wrong took place in Nebraska, the location of “the last event necessary to make the actor liable.”

With regard to Nebraska, “the relevant statute does appear to give businesses greater latitude to record conversations of their employees than do some other single-consent states.” Nevertheless, the statute still requires notice to be given to employees when a policy of “service observing or random monitoring” is to be used. To the argument that as a practical matter the application of California law would require Omni to change its policies for all incoming calls, the Court found that plaintiffs have raised genuine issues of material fact as to the feasibility of determining incoming callers’ location and state of residency. Moreover, Omni’s own proffered evidence that being informed of recording at the beginning of a call would not change callers’ behavior, undermined their contention that Nebraska’s pro-business interests would be severely hampered by application of CIPA. Overall,

the Court finds that the interests of California in the privacy of its consumers would be affected more by the application of Nebraska law than Nebraska’s pro-business interests would be affected by the application of California law.

Given California’s clearly expressed interest in protecting its residents from secretly recorded phone calls, which the California Supreme Court has found would be seriously impaired by the application of less protective privacy law, and the less clear showing that Nebraska’s interests would be severely impaired by application of California law, the Court found California law applicable to this case.

Dormant Commerce Clause

Omni contended that applying § 632.7 as plaintiffs urged would violate the dormant Commerce Clause of the United States Constitution. Omni first contended that application

of § 632.7 to these facts would effect direct regulation of extraterritorial commerce, constituting a per se violation of the dormant Commerce Clause. Plaintiffs responded that there is no direct extraterritorial regulation here because the telephone calls at issue do not take place wholly outside California. They further argued that § 632.7 does not discriminate in any way because it treats out-of-state and in-state businesses the same: both must obtain consent before recording calls from California customers.

The Court agreed with plaintiffs that this case does not merit strict scrutiny under the dormant Commerce Clause. “First, § 632.7 does not discriminate facially, purposefully, or practically against out-of-state commerce. Omni appears to concede that the statute does not discriminate facially or purposefully, and there is case law to that effect.” “Nor does the statute have a discriminatory effect.” Nor does § 632.7 directly regulate out-of-state commerce in violation of what has been called the “extraterritoriality doctrine.” California law applied to Omni’s telephone conversations with Californians, “and out-of-state companies that conduct telephone business with California consumers have been on notice of this at least since *Kearney* was decided in 2006.” This case was therefore different from cases cited by Omni in which a state “projected its legislation” into other states to affect conduct with no California nexus.

The calls at issue involved telephonic connections between California and Nebraska, and it was Californians who allegedly had their conversations recorded without forewarning. Although the portability of mobile phone numbers may make it difficult to know with certainty whether a caller is indeed calling from or residing in California, viewing the evidence in the light most favorable to plaintiffs as the Court was required to on a motion for summary judgment, there was at least a triable issue of fact as to whether it would be “futile” for Omni to differentiate among Californian and non-Californian callers.

Moreover, legislation that may cause businesses to decide to conform nationwide conduct to meet the requirements of a given state does not necessarily constitute direct regulation of out-of-state commerce. “Courts have held that when a defendant chooses to manufacture one product for a nationwide market, rather than target its products to comply with state laws, defendant’s choice does not implicate the commerce clause.” The Ninth Circuit has recently held that “regulation with reference to local harms” does not constitute extraterritorial regulation under the Commerce Clause merely because that regulation creates incentives for businesses to alter out-of-state activity. *Rocky Mountain Farmers Union*, 730 F.3d at 1101–06 (holding that California fuel standards taking into account “lifecycle” emissions did not “control conduct wholly outside the state” despite arguments that the standards forced plaintiffs to conform out-of-state conduct to California law). Similarly, § 632.7 regulates only calls with a nexus to California and has the purpose of preventing

privacy harms to Californians, even if it might create incentives for Omni to alter its behavior nationwide.

Despite Omni's argument that § 632.7's application to Omni's conduct provides "no real benefit whatsoever," the Court found persuasive the California Supreme Court's reasoning that refusing to apply the law to similar conduct would "significantly impair the privacy policy guaranteed by California law." Against these real local interests, the Court did not find that Omni has shown clearly excessive burdens on interstate commerce.

Excessive Damages

Omni next argued that the statutory damages sought by plaintiffs are unconstitutional under the Excessive Fines Clause, U.S. Const. amend. VIII, and due process principles. The Excessive Fines Clause "is inapplicable where, as here, civil damages are sought in a lawsuit between private parties." "[A]t this stage of the proceedings, there is simply nothing in the record that would permit the court to apply" the reasonableness guideposts urged by Omni "in an informed manner," and any inquiry would be "speculative, based on a potential statutory maximum award rather than an actual jury verdict."

§ 632.7's Applicability To Call Participants

Omni also argued that § 632.7 does not apply to call participants based on differences between the language in that provision and § 632. Specifically, § 632 holds liable anyone who "eavesdrops upon or records" a telephone communication, and § 632.7 imposes liability on anyone who "intercepts or receives and records" a cellular telephone call. However, the Court agreed with the decisions cited by plaintiff, and found that § 632.7 prevents a party to a cellular telephone conversation from recording it without the consent of all parties to the conversation. "This interpretation flows from the clear and unambiguous language of the statute." As a matter of common usage, the participants in a conversation "receive" communications from each other. "This alone suggests that § 632.7 should not be limited to situations in which unknown third parties record a conversation."

* * *

Jung v. Chorus Music Studio, No. 13–CV–1494 (CM)(RLE) (S.D. N.Y. Sep. 11, 2014)

Federal Court Holds That a CFAA Counterclaim Would Not Be Futile Even Though the Proposed Counterclaim Did Not Allege Unauthorized Access

The Courts of Appeals are split as to whether the Computer Fraud and Abuse Act (CFAA) creates liability whenever an employee misuses a workplace computer by using information contained on it for improper purposes or whether, more narrowly, it creates liability only when the employee accessed a computer that he or she was altogether prohibited from using. In opposing the filing of a CFAA counterclaim as futile, the plaintiffs in this case argued that the Second Circuit had embraced the narrow view of the CFAA as creating liability only for unauthorized access to an employer's computer. The Court, however, read the Second Circuit precedent as inconclusive on this issue and allowed the proposed counterclaim to be filed against a named plaintiff who was authorized to use the computer at issue but who allegedly misused the information he found on it for his own personal business venture. The Court thus suggested that it may agree with the broad view of the CFAA as creating liability for misuse of employer information, although the Court did not squarely rule on that issue in this opinion.

Background

Plaintiffs were waiters and busboys at Defendants' karaoke lounge, Chorus Karaoke. At his deposition, Hong testified that:

[T]here was an occasion when the shop had to change the computer and at that time, the manager instructed me to back up the information that had been stored in the previous computer in a file. So I forwarded the content to my own e-mail address when the computer was removed and I stored the information that had been installed in my e-mail account and that was it. I never opened them.

Defendants alleged that, in April 2013, plaintiffs initialed their own business venture, Club 88 NY. Defendants asserted that plaintiffs used defendants' customer list and other proprietary information taken by Hong from Defendants' computer to promote their new venture, citing Exhibit G, which appears to be a printout from the website of Club 88 NY. Plaintiffs disputed both of these allegations. Defendants sought leave to amend their complaint to add a Computer Fraud and Abuse counterclaim against the plaintiffs.

Defendants' Proposed Counterclaim Under The CFAA Is Permitted Regarding Plaintiff Except Hong

Plaintiffs asserted that defendants have alleged only that Hong misused the information in Chorus's business computer by transferring it to his own email account, and had not alleged that he did not have authorization to access the computer. Plaintiffs argued that courts

in this district had interpreted the CFAA as prohibiting only unauthorized access to information, and not misuse of information. “Although the Second Circuit has not ruled on the issue, Plaintiffs assert that the Second Circuit’s decision in *Nexans Wires S.A. v. Sark–USA, Inc.* supports a narrow interpretation of the CFAA. 166 F. App’x 559, 562 (2d Cir.2006) (denying remedy under CFAA for revenue lost due to misappropriation of information).”

Plaintiffs’ arguments were deemed unpersuasive. In their proposed First Amended Answer, defendants asserted that “Plaintiff Hong intentionally stole electronic proprietary information when he transferred all electronic files from Chorus’ business computer to his personal e-mail without authorization.” Defendants also asserted that plaintiff Hong was “not needed or asked, at any relevant time to . . . access the business computer.” Defendants alleged misuse or misappropriation of electronic information but not unauthorized access. The Second Circuit has not ruled on what elements constitute violations of the CFAA, and not all courts in this district have adopted plaintiff’s narrower interpretation of the CFAA. In *Calyon v. Mizuho Secs. USA, Inc.*, for example, the court reasoned that the plain language of the statute seems to contemplate that “without access” and “exceeds authorized access” would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer and found that employees who transferred information from their employer’s computer to their personal email accounts before starting work at another company violated the CFAA. No. 07–CV–2241 (RO), 2007 WL 2618658, at *1 (S.D.N.Y. July 24, 2007). “Because Defendants’ proposed counterclaims need only be plausible to be considered not futile. *N.H. Ins. Co. v. Total Tool Supply, Inc.*, 621 F.Supp.2d 121, 124 (S.D.N.Y.2009),” the Court found that Defendants’ proposed claims would be allowable against Hong.

Plaintiffs also argued that defendants had not plausibly alleged that Hong’s actions “caused damage or loss in excess of \$5,000 in one year to one or more persons.” 18 U.S.C. §§ 1030(c)(4)(A)(i) (I)–(V). Defendants, however, had allegedly spent at least \$5,000 to respond to the theft and assess the damage within the meaning of the CFAA.” (Def. Decl. Ex. A ¶ 81.) Plaintiffs further asserted that it was not plausible that Defendants could have incurred a loss of \$5,000 or more, but plaintiffs had not shown that Defendants’ claim regarding damages was implausible. “Accordingly, Defendants’ CFAA claim is not clearly futile against Hong.”

Defendants’ CFAA claim against the other named plaintiffs, however, was deemed futile. Defendants asserted that the other named Plaintiffs conspired with Hong to use the proprietary information Hong took from Defendants’ business computer to promote their new business venture. To support their conspiracy allegation, defendants made a number of conclusory allegations, including: (1) “Plaintiff Hong conspired with other named

Plaintiffs in the main action to take Chorus' proprietary information for use in a lawsuit against Defendants while they were still employed at Chorus", (2) "Plaintiffs aided and abetted Plaintiff Hong in the theft of Chorus' electronic proprietary information. . . ", (3) "Plaintiffs sold the subject customer lists to third parties and unjustly enriched themselves", and (4) "Plaintiffs contacted or solicited customers on the stolen customer list to promote their business Club 88 N.Y. and other business ventures or agreements they had." "These conclusory allegations cannot be considered in determining whether Defendants' proposed counterclaims state a claim for relief. *Iqbal*, 556 U.S. at 678."

Defendants also relied on the fact that the other named Plaintiffs quit Chorus Karaoke on the same day, that Hong discussed quitting his employment at Chorus Karaoke with the other named Plaintiffs a week before he quit, and that all of the named Plaintiffs' names appeared on the advertisement for their alleged new business venture. Club 88, and that Plaintiff HaeYoung Lee organized this business venture. Even "assuming all of Defendants' allegations are true, they do not support a conclusion that the other named Plaintiffs conspired with Hong." "Defendants do not allege that the other named Plaintiffs had any connection to the alleged unauthorized transfer of Defendants' proprietary information." Defendants merely alleged parallel conduct by the named plaintiffs, which is not sufficient to establish conspiracy. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556–57 (2007). "Accordingly, Defendants' allegations do not state a claim against the other named Plaintiffs under the CFAA, and Defendants' counterclaim against them would be futile."

* * *

DATA BREACH; ARTICLE III STANDING; CONCRETE; CREDIT CARD; MOTION TO DISMISS

Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735 (N.D. Ill. Sep. 16, 2014)

Federal Court Holds That Department Store Customers Whose Credit Card Information Was or May Have Been Stolen Lacked Standing Because They Had Not Incurred a Concrete Injury

The Court held that department store customers whose credit card information was or may have been stolen lacked standing to sue the department store. Even with respect to those customers whose data actually was stolen and who had fraudulent charges made to their credit cards, there was an insufficiently concrete injury for Article III standing, because those customers presumably had those fraudulent charges removed from their accounts and were not forced to pay them. The time and effort dealing with fraudulent charges was dismissed by the Court as de minimis and insufficient to qualify as a concrete injury.

The Court also was unpersuaded by the plaintiffs’ “creative” theory that they overpaid for the defendants’ products because the prices for those products should have included defendant’s costs of providing adequate data security, which in fact was not provided. The Court did hint that more specific allegations of harm from incurring fraudulent charges on the part of individual plaintiffs might be sufficient to establish standing.

Editor’s Note: To the extent that this opinion holds that a plaintiff lacks a concrete injury that would confer standing even if his or her card personal information was stolen and he or she incurred fraudulent charges and had to take measures to remove those charges, it seems to establish an extremely high standard for standing in breach of data security cases. In particular, the Court seems remarkably dismissive of the notion that dealing with fraudulent charges is a genuine cost to the victims of theft of credit card information. It remains to be seen whether, if the plaintiffs in an amended complaint detail the hardships imposed by dealing with fraudulent charges, the Court will re-consider its holding and make more room for standing in data breach suits. This opinion could be a very helpful precedent for businesses seeking dismissal on standing grounds of suits based on breaches of data security.

Background

In 2013, hackers breached defendant’s servers, resulting in the potential disclosure of 350,000 customers’ payment card data and personally identifiable information. At some point following the breach, it became clear that, of the payment cards that may have been affected, at least 9,200 were subsequently used fraudulently elsewhere. Plaintiffs were among the 350,000 customers, and they brought this lawsuit against defendant for failing to adequately protect against such a security breach, and for failing to provide timely notice of the breach once it happened.

Plaintiffs asserted that they had been injured in that defendant’s alleged misconduct exposed them to an increased risk of future fraudulent credit card charges, and an increased risk of identity theft. Plaintiffs also asserted present injuries, including the loss of time and money associated with resolving fraudulent charges, the loss of time and money associated with protecting against the risk of future identity theft, the financial loss they suffered from having purchased products that they wouldn’t have purchased had they known of defendant’s misconduct, and the loss of control over and value of their private information. Defendant argued that none of these asserted injuries was sufficient to establish Article III standing.

No Article III Standing

Three courts in this District have recently taken up the question of standing and the increased risk of future harm plaintiffs encounter in the context of such cyber-attacks. *See*

Moyer v. Michaels Stores, Inc., 2014 WL 3511500 (N.D.Ill. July 14, 2014); *Strautins v. Trustwave Holdings, Inc.*, 2014 WL 960816 (N.D.Ill. March 12, 2014); *In re Barnes & Noble Pin Pad Litigation*, 2013 WL 4759588 (N.D.Ill. Sept. 3, 2013). The *Strautins* Court concluded that the Supreme Court's decision in *Clapper* implicitly overruled a facially more relaxed standard for evaluating standing in this context articulated in *Pisciotta v. Old Nat. Bancorp.*, 499 F.2d 629, 634 (7th Cir. 2007). In *Pisciotta*, the Court held that

the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions.

The *Moyer* Court concluded that there was room for *Clapper* and *Pisciotta* to co-exist. See *Moyer*, 2014 WL 3511500, at *6.

The Court explained that the “certainly impending” standard pre-dates *Clapper*, see *Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979), though the *Clapper* Court itself acknowledged that the underlying facts called for an “especially rigorous” standing inquiry, see *Clapper*, 133 S.Ct. at 1147. “Those facts are not present here.” Read literally, *Pisciotta* could be understood to have held that *any* marginal increase in the risk of future injury is sufficient to confer Article III standing. That would be difficult to square with *Clapper*, which sets a threshold that an increase in the risk of harm must meet in order to confer standing. “But in my view, it is hard to imagine that that is what the *Pisciotta* Court intended, and such a literal reading of *Pisciotta* would not be reasonable.” “The *Pisciotta* Court raised the issue of standing *sua sponte*, and was not prompted to thoroughly discuss it.” Though it does not expressly say so, *Pisciotta* was constrained by the “certainly impending” standard, first articulated 27 years earlier in *Babbitt*, and the Court “read that standard into the opinion.”

Here, the overwhelming majority of the plaintiffs alleged only that their data *may* have been stolen. In this sense, the instant case was like *Strautins* and *Barnes & Noble*. Unlike *Strautins* and *Barnes & Noble*, however, plaintiffs also alleged that 9,200, or approximately 2.5% of these customers have actually had fraudulent charges appear on their credit cards. In other words, these customers' data were actually stolen and were actually misused. But it was “not clear” to the Court that the “fraudulent charge” injury alleged to have been incurred by the 9,200 customers, or, *a fortiori*, the risk that the same injury may befall others among the 350,000 customers at issue, was an injury sufficient to confer standing. To satisfy their burden to establish standing, plaintiffs must show that their injury is concrete, particularized, and, if not actual, at least imminent. Here, as common experience might lead one to expect, plaintiffs have not alleged that any of the fraudulent charges

were unreimbursed. “On these pleadings, I am not persuaded that unauthorized credit card charges for which none of the plaintiffs are financially responsible qualify as ‘concrete’ injuries. *See Barnes & Noble*, 2013 WL 4759588, at *6; *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, *8 (S.D.N.Y. June 25, 2010).” “Without a more detailed description of some fairly substantial attendant hardship, I cannot agree with Plaintiffs that such “injuries” confer Article III standing.”

Plaintiffs also claimed the time and money allegedly spent toward mitigating the risk of future fraudulent charges and identity theft constitutes injury sufficient to confer standing. The cost of guarding against a risk is an injury sufficient to confer standing only if the underlying harm the plaintiff is seeking to avoid is itself a cognizable Article III injury. *See Moyer*, 2014 WL 3511500, at *4 n. 1. “As discussed above, however, on these pleadings I am not satisfied that either of the future injuries claimed in the complaint are themselves sufficient to confer standing.” The “fraudulent charge” injury, absent unreimbursed charges or other allegations of some substantial attendant hardship, “is not in my view sufficiently concrete to establish standing.” In any event, the complaint contained no meaningful allegations as to what precisely the costs incurred to mitigate the risk of future fraudulent charges were. Generally, when one sees a fraudulent charge on a credit card, one is reimbursed for the charge, and the threat of future charges is eliminated by the issuance of a new card, perhaps resulting in a brief period where one is without its use. “If the complaint is to credibly claim standing on this score, it must allege something that goes beyond such *de minimis* injury.”

Plaintiffs also asserted that they paid a premium for the retail goods purchased at Defendant’s stores, a portion of which defendant was required to allocate to adequate data breach security measures. Because defendant did not do so, plaintiffs alleged, plaintiffs overpaid for their respective purchases and would not have otherwise made them. “As Plaintiffs would have it, this financial injury establishes standing.” The Court found this argument creative, but unpersuasive. “In my view, a vital limiting principle to this theory of injury is that the value-reducing deficiency is always intrinsic to the product at issue.” Under Plaintiffs’ theory, however, the deficiency complained of is extrinsic to the product being purchased. To illustrate the problem this creates: suppose a retail store does not allocate a sufficient portion of its revenues to providing adequate in-store security. A customer who is assaulted in the parking lot after patronizing the store may well have a negligence claim against the store owner. But could he or she really argue that she overpaid for the products that she purchased?

Or even more to the point: even if no physical injury actually befell the customer, under Plaintiffs' theory, the customer still suffered financial injury because he or she paid a premium for adequate store security, and the store security was not in fact adequate.

Finally, "I am also unpersuaded by Plaintiffs' claim to standing based on the loss of control over and value of their private information," because the injury as pled was not sufficiently concrete.

* * *

Best of the Blogs

CONTENT REGULATION

Three D, LLC d/b/a Triple Play Sports Bar and Grille and Jillian Sanzone / Spinella, No. 34-CA-012915 (NLRB, Aug. 22, 2014)

NLRB Invalidates Employer's Blogging Policy And Reverses Firing Based On Facebook Posts

Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

This is another NLRB Facebook firing case. The employer is a bar and restaurant whose employees were chatting on Facebook about owing amounts in taxes allegedly as a result of paperwork mishaps on the employer's part. LaFrance, a former employee posted:

[m]aybe someone should do the owners of TriplePlay a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money.....Wtf!!!!

The following responses ensued:

You owe them money..that's fucked up [a Facebook friend and customer]

I FUCKING OWE MONEY TOO! [current employee]

The state. Not Triple Play. I would never give that place a penny of my money. [The owner] fucked up the paperwork...as per usual [the former employee who started the thread]

Yeah I don't go to that place anymore. [Facebook friend and customer]

It's all Ralph's fault. He didn't do the paperwork right. I'm calling the labor board to look into it bc he still owes me about 2000 in paychecks. [the former employee]

...

[Spinella, another employee, did not comment, but clicked the "like" button.]

I owe too. Such an asshole. [Sanzone, another employee]

Some time later, Sanzone was advised that she was being let go. While she thought at first that her firing was a joke, the company reiterated and told her she was being terminated for disloyalty.

Spinella, following what appeared to be a lengthy interrogation on the mechanics of Facebook, was also let go (while the parties discussed the “like” button at length, Spinella was purportedly terminated for other reasons).

The employer did not relent, and unleashed its lawyers on Sanzone and LaFrance, demanding that they retract the Facebook comments. Sanzone could not delete the comment that was posted to LaFrance’s page and asked LaFrance to delete Sanzone’s comment, which she did. LaFrance posted a retraction in response to the letter she received, and the lawyers pressured Sanzone to do the same, arguing that deletion is not the same as retraction. [Whatever sympathy I had for the employer when I first read the facts has pretty much run dry at this point.]

The employer also had an internet/blogging policy that read as follows:

The Company supports the free exchange of information and supports camaraderie among its employees. However, when internet blogging, chat room discussions, e-mail, text messages, or other forms of communication extend to employees revealing confidential and proprietary information about the Company, or *engaging in inappropriate discussions about the company, management, and/or co-workers*, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment. Please keep in mind that if you communicate regarding any aspect of the Company, you must include a disclaimer that the views you share are yours, and not necessarily the views of the Company. In the event state or federal law precludes this policy, then it is of no force or effect. [emphasis added]

The board concludes that the employees in question were engaged in concerted activity when they participated in the Facebook discussion. Wages and tax issues are directly related to employment, and the fact that the discussions took place on Facebook does not change their character as collaborative. The board also says that Spinella’s use of the like button was sufficient to convey his participation. The key question was whether the comments lost their protective character and crossed over into the territory of disparagement.

Applying the balancing test used for out-of-workplace interactions, the board says the employees’ comments did not cross the line. In doing so, the board looks to the context of the discussions and the fact that the statements were not made to the general public (the court cites to the vague privacy settings but notes that the page was in the nature of a semi-closed discussion). The board also says that the particular speakers in question cannot be responsible for the comments of others, except for those that they specifically adopted. While some participants may have crossed the line and have engaged in unprotected activity, this does not transform the nature of the others’ participation. The board thus concludes that the discharges violated the Act.

The board also looks at the employer's internet and blogging policy and finds it problematic. In particular, the putative prohibition on "inappropriate discussions about the company, management, and/or coworkers" on social media could be viewed by employees to chill protected activity. Indeed, the discharges in question reflect the employer's authoritative interpretation of the scope of the policy, and confirm that it could reasonably be interpreted to encroach on the sphere of protected activity. One board member dissented from this last finding.

Another case where the "like" button has legal consequences. (Cf. [Bland v. Roberts](#).) I love it! Given the decidedly ambiguous nature of "likes" (it's not uncommon for people to "like" obituary posts) it seems petty on the part of employers to terminate someone on the basis of liking a post. Perhaps the board had a similar instinct.

The case also reflects the disparate rules various types of employers face in disciplining or terminating their employees. As we've blogged, outcome of the public employee cases are tough to predict. What appears to be in a statement of public interest in one case is treated as mere (and possibly disruptive) venting in another. It's similarly tough to ascertain a clear rule for private employers. Even as a private employer, if your reason for discharge relates to something that may touch on the terms of employment (and we've seen examples of how this can be broadly construed), you should tread carefully. On the other hand, numerous cases have approved employee firings based on statements that call into question their underlying judgment and decision-making ability (e.g., teachers, nurses, administrative adjudicators). [From an employee's perspective, if you're going to complain, don't do it about your customers; kvetch about your boss instead?] It's also interesting and somewhat comforting that the board took the trouble to separate out statements made by the individual employees and others—mere participation in a discussion even when others engage in non-protected activity or cross the line is not enough to disqualify you from protection.

Even more interesting than the firing ruling is the finding regarding the no-blogging/internet usage policy. I don't have a sense of clear rules. (See a prior post from 2011 on similarly muddled guidance: "[Overreacting Guidance for Social Networking Du Jour — NLRB Edition](#)".) Perhaps a scaled back policy that references things like trademark usage, trade secrets, etc. (clear cut legal rules) is prudent, and any attempt to vaguely prohibit inappropriate, offensive, disparaging discussions should be avoided?

Related posts:

[Texas Court of Appeals Rejects Privacy Claims Based on Facebook Firing – Roberts v. Craftily](#)

Teacher's Semi-Racy Facebook Photo Doesn't Justify Firing – In re Laraine Cook

Do Employers Really Tread a Minefield When Firing Employees for Facebook Gaffes?

Employee's Discrimination Claim Can't be Salvaged by Coworker's Allegedly Inappropriate Facebook Post — Brown v Tyson Foods

More Proof That Facebook Isn't The Right Place To Bitch About Your Job–Talbot v. Desert View

Facebook Post Isn't Good Reason To Remove Attorney From Probate Court Case Assignment List

Demoting Police Officer for Posting Confederate Flag to Facebook Isn't First Amendment Violation

Nurse Properly Fired and Denied Unemployment Due to Facebook Rant

Police Officer's Facebook Post Criticizing Her Boss Isn't Protected Speech–Graziosi v. Greenville

Facebook Complaints About Boss's Creepy Hands Can't Salvage Retaliation/Harassment Claims

Facebook Rant Against 'Arial' Font Helps Reverse Sex Offender Determination

Employee Termination Based on Mistaken Belief of Facebook Post Authorship Upheld — Smizer v. Community Mennonite Early Learning Ctr.

Social Worker's Facebook Rant Justified Termination — Shepherd v. McGee

Police Officers Lean on School to Fire Social Worker for Facebook Post—and May Have Violated First Amendment

Police Officer's Facebook Venting Isn't Protected By The First Amendment–Gresham v. Atlanta

Court Upholds Doocing For Snarky Facebook Post — Rodriquez v. Wal-Mart

Employee's Privacy Claim Based on Allegedly Improper Access to Facebook Post Fails — Ehling v. Monmouth-Ocean Hosp.

University May Be Liable for Improper Access to Student's Facebook Photos – Rodriguez v. Widener Univ.

Facebook Entry and Blog Post May Support Retaliation Claim – Stewart v. CUS Nashville

Employee Terminated for Facebook Message Fails to State Public Policy Claim — Barnett v. Aultman

* * *

Turner v. Temptu Inc., No. 13-3440 (2d Cir. Sept. 23, 2014)

Jointly Editable Online Document Doesn't Provide Evidence of Contract Formation

Eric Goldman

<http://www.blog.ericgoldman.org>

© 2014 Professor Eric Goldman. Professor Goldman teaches at the University of Santa Clara Law School and is the Director of the school's High Tech Law Institute.

The litigants discussed working together to launch a new product in the marketplace. As seems to be inevitable in situations like this, the parties' relationship fell out. Trying to salvage something from the situation, Turner alleged the parties had formed a joint venture. As supporting evidence for the joint venture agreement, Turner pointed to conversations between the parties in a jointly edited "blog," although what made it a "blog" wasn't clarified in the opinion. Instead, it sounds a lot more like a shared Google document or similar jointly editable document. Either way, the court says that the "blog" evidence is insufficient to show that a contract formed (citations omitted):

Turner argues that a blog edited by herself, Benjamin, and Roger Braimon constituted a binding joint venture agreement. Turner testified that this blog—an "editable" working document that was "constantly changing and modifying"—contained the terms of their oral partnership agreement and "served as a living document for [them] to write, edit, and memorialize [their] discussions."...

Although the parties' blog contained a number of possible contract terms, Turner admitted at her deposition that many of these had not been finalized, indeed, several of them were marked "to be determined." Turner also acknowledged her understanding that the alleged agreement was not finalized as late as April 2007, when "still some discussion [] needed to take place with respect to the contents of [their] contract." Also in April, Braimon sent an e-mail to a lawyer, stating that the parties had yet to "establish a contract" and were still "undecided" even on the "actual product" they would develop together. Perhaps most telling is that, when asked at her deposition if the parties had ever finalized their agreement, Turner responded, "No. I would have loved to." Given this record, no reasonable jury could find that the parties manifested the requisite intent to enter into a binding partnership agreement.

Whether it's a blog or a Google doc, there's no reason why a jointly editable document couldn't be used to form a contract even if there's no magic moment when ink hits paper. The freely editable nature of the document might raise questions about which version was "final" and if the evidence can be properly authenticated. On the other hand, if the document provides a revision history allowing for the parties to easily trace the what/when of

each iteration in the conversation, it might actually be more evidentiarily reliable than a string of emails or other types of parol evidence.

* * *

CONTENT REGULATION; DERIVATIVE LIABILITY

Jane Doe No. 14 v. Internet Brands, Inc., No. 12-56638 (9th Cir. Sept. 17, 2014)

9th Circuit Creates Problematic “Failure To Warn”

Exception to Section 230 Immunity

Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

Doe sued Internet Brands, Inc., the owner of Model Mayhem, alleging that two unrelated individuals drugged and assaulted her (and recorded her for a pornographic video). It’s unclear precisely how the assailants used Model Mayhem, but the court merely says that they “used the website to lure [Doe] to a fake audition.” Doe asserted a negligence claim against Internet Brands, alleging that it knew of the specific assailants in question and had a duty to warn her.

Specifically, Internet Brands had purchased Model Mayhem in 2008, and later sued the sellers for failing to disclose the potential for civil liability arising from the activities of these same two assailants. A copy of Doe’s complaint, which lays out the chronology, is here: [\[pdf\]](#). The two individuals were arrested in 2007, Internet Brands bought the site in 2008, and sued the sellers in 2010. By August 2010, Doe claims that Internet Brands had the requisite knowledge. [\[Kash Hill\]](#) gets into more detail about the case’s background.]

The district court **dismissed** on the basis of Section 230. See [Internet Brand’s motion to dismiss](#).

The Ninth Circuit reverses, concluding that Section 230 does not bar Doe’s duty to warn claim. According to the court, this isn’t a case that’s based on Model Mayhem’s failure to remove content. In fact, the assailants are not even have alleged to have posted any content (“The Complaint alleges only that “Jane Doe” was contacted by [the assailants] through ModelMayhem.com using a fake identity.”). In contrast to being a case about the removal of third party content, the court says it’s about content (i.e., a warning) that Model Mayhem itself failed to provide.

The court also says that imposing failure to warn liability is consistent with the overall purposes of Section 230, which as set forth in sections (c)(1) and (b) encourages

self-regulation of offensive content and seeks to protect the free-flow of information via intermediaries. [I don't know what the word is for when someone cites to authority that's the exact opposite of what it is cited for, but this is what happened here.] [Eric's thoughts: reading comprehension failure? judicial activism? intellectual dishonesty?]

Sure, imposing a duty to warn imposes some costs on an internet business and may have a "marginal chilling effect". However, the court says that finding the claims against Model Mayhem are barred by Section 230 would stretch Section 230 beyond its "narrow" language and purpose, and would give Model Mayhem a "get out of jail free card" which is not what Section 230 was intended to do. Model Mayhem is a "publisher or speaker" of third party content and this is the but-for cause of her injury, but:

[p]ublishing activity is a but-for cause of just about everything Model Mayhem is involved in. It is an internet publishing business.

In other words, interpreting Section 230 broadly would make it pretty tough to bring any sort of claim against Model Mayhem.

The court does note that it is not expressing any opinion on the merits of the duty-to-warn claim.

This is a bombshell ruling and is similar in some ways to [Garcia v. Google](#). Both involve a sympathetic plaintiff and a bad (in this case, horrific) set of facts, but both rulings also totally diverge from established precedent, and both create gaping doctrinal holes. (Here, there were a bunch of cases dealing with the exact same fact pattern that go the other way, e.g., [Doe v. MySpace](#); [Beckman v. Match.com](#); [Doe II v. MySpace](#).)

There are a lots of unsatisfying answers and things that leave you scratching your head, but perhaps the biggest qualm is that Doe would have likely lost on the merits, so it seems unnecessary for the court to do a total 180 from existing precedent and create what is a gaping hole in Section 230. First, Doe's duty to warn claim depends on finding a "special relationship", and courts typically find that websites do not have special relationships with users. (See, e.g., [Rosenberg v. Harwood](#), the Google maps case; and [the Armslist case](#).) It's unclear what the basis is for one here. Second, Model Mayhem is the provider of an information (content) product and courts are reluctant, for First Amendment reasons, to impose liability against publishers [based on mere negligence principles](#). In other words, even without Section 230 (say, if this were a case involving printed classified ads), Doe would have a tough time making a case.

As to the Section 230 analysis, it is tough to grok the court's distinction between claims based on a disclaimer or warning that the provider is required to publish (not barred by

Section 230) and claims based on user-submitted content itself (barred by Section 230). This is the type of creative workaround that countless plaintiffs have tried and courts have consistently rejected. Perhaps an absurd scenario, but you could stretch the court's logic to say that while websites can't be held liable for hosting defamatory content, they can be held liable for failing to provide disclaimers about that content.

If you accept the argument that Model Mayhem has an obligation to warn (seemingly about specific activity), doesn't this mean that all intermediaries have an obligation to warn about possibly harmful users, including content that such users may post? For that matter, do websites have a duty to warn about all manner of possible dangers that users may be exposed to when communicating with others via a website? This also brings to mind another point of the court ruling: it takes pains to say that liability in this case is not based on content the assailants made available, so Model Mayhem was used solely as a channel for communications. This means that sites that merely allow users to chat with each other could also be on the hook for failure to provide warnings about dangerous users?

One obvious practical effect of the ruling will be that websites that have undertaken measures to screen and get rid of problem users (e.g., sex offenders) now have a serious disincentive to do so, since Section 230 no longer is a bar to failure to warn claims. If it comes across a specific user with a past that is indicative of dangerousness and fails to warn, it may be on the hook. It's possible that a website or network will have to warn users about all possibly dangerous users that it comes across through any means (e.g., through its screening process, user disputes, unsolicited emails from other users, warrant requests, email scans). To the Facebooks and Googles of the world, this is probably a staggering burden. It's not only significant for social networks, but also for sharing economy sites.

The ruling also raised many practical questions about implementation. How exactly a website would provide notice to users about other specific users—the court suggests this would take the form of a “post or email warning” but does this mean that users will now be barraged with myriad warnings about possible dangers that lurk in websites? What is the form of the warning? I assume a standard disclaimer (**which Model Mayhem likely had in place**) is insufficient; it seems like the court was talking about websites having to provide specific warnings. Would sending a warning put a site at greater risk if the warning turns out to be inadequate in form or substance? Could networks be at risk from the subjects in question (perhaps for defamation claims) when they send this type of a warning? [Eric's answer to that last question: yes] So many questions here.

I'm not sure what the 9th Circuit has against Section 230: **Roommates**; **Barnes v. Yahoo**; and now this. (It seems like Roommates and Barnes have not been

exploited by the plaintiffs, but this ruling will be different.) The ruling diverges from the clear trend, which even in recent cases has continued to recognize robust immunity ([Klayman](#); [the Dirty](#); [NJ/WA Backpage rulings](#)). I'm guessing there will be a request to rehear this case, along with interest and participation from a long list of amici.

Eric's Comments: It's so hard to take this opinion seriously because the court's hack job was so transparent. As Venkat explains, the plaintiff's failure-to-warn claim is almost certainly doomed on its prima facie elements. A standard customer-vendor relationship isn't a "special" relationship for negligence purposes, and the underlying event triggering the lawsuit was a third party's criminal act that ought to cut off ModelMayhem's contributing causation. Could you imagine a print newspaper being negligent for failing to warn any job-seeking advertisers that rapists were reading the classified ads? In fact, the court repeatedly notes that it wasn't trying to prejudice the lower court's further proceedings on the prima facie case, but this sends a pretty strong hint to the district court judge that the Ninth Circuit thinks this case should fail. So knowing that its ruling wouldn't affect the ultimate outcome, this Ninth Circuit panel felt emboldened to muck around with Section 230. Yet, if a case is DOA anyway, we want to find a limiting principle—like Section 230—that screens it out quickly. Recall the [Roommates.com](#) case, where [Roommates.com won a 230 dismissal](#) at the trial court in 2004. 8 years later, in 2012, the Ninth Circuit [says there never was a valid claim](#) because the case never satisfied its prima facie elements. Justice was served in the sense that the dismissal was ultimately grounded on the legally correct principles, but 8 extra years of litigation is hardly justice being served. That's not a reason to distort Section 230's scope, but it is a good reason why appellate court panels should be extra-cautious when it comes to Section 230.

The adverse consequences from this opinion go beyond just this case. Similar to [the PDX v. Hardin case](#) I recently discussed, the court rips open a hole in Section 230's immunity for any situation where the plaintiff pleads a failure-to-warn claim. Hmm, I wonder how plaintiffs might respond...is it possible they'll plead a failure-to-warn claim in every complaint that might otherwise be preempted by Section 230? After all, there's always *something* more that websites could warn their users about. For example, if a Yelp reviewer gets sued for posting a defamatory review, the user could sue Yelp for "failure to warn" because Yelp knows its authors are sometimes sued for defamation. Or if Larry Klayman is unhappy about finding anti-Semitic content on Facebook, he can sue Facebook for failing to warn him that he might encounter anti-Semitic content. Or if a boyfriend assaults a girlfriend because of what she said in her Facebook post, the girlfriend could sue

Facebook for failing to warn her that sometimes Facebook status posts lead to domestic violence.

Websites could try to mitigate this possibility by disclosing every risk they can possibly think of. Is that the world we want? We're already overwhelmed by long online user agreements that no one reads, and we're already overwhelmed with so many warnings and disclosures in our lives that we can't process and follow them all. If we take this opinion seriously, it will compound the existing over-disclosure problem. Worse, it will provide little or no real value to users given that few of them read the website disclosures (and fewer still will read them if they further balloon in length as this opinion encourages).

If Section 230 is categorically inapplicable to the failure-to-warn claim, the examples I gave above could survive a motion to dismiss—even though we know that most, if not all, of the failure-to-warn claims are going to fizzle out eventually. So the opinion imposes significant and needless costs on defendants and the court system to adjudicate unmeritorious claims. This runs contrary to the warnings of the *Roommates.com* case, which said:

Websites are complicated enterprises, and there will always be close cases where a clever lawyer could argue that something the website operator did encouraged the illegality. Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites, fighting off claims that they promoted or encouraged—or at least tacitly assented to—the illegality of third parties.

The opinion was embarrassingly lackadaisical about this inevitable unwanted consequence. If Section 230 doesn't work, but failure-to-warn does, the plaintiffs' backdoor claims undermine the overall immunity effect of Section 230. It's as if the opinion author didn't understand the substitutive effects between a "failure to warn" claim and Section 230-preempted claims.

The opinion also didn't properly address the precedent. We've seen numerous "negligence" claims preempted by Section 230, going all of the way back to *Zeran v. AOL*, which was a negligence case, not a defamation case. The opinion's most obvious omission was the [Fifth Circuit's Doe v. MySpace case](#), also involving an offline sexual assault facilitated by the UGC site's online publication tools. In that case, the court said the plaintiff's "case is predicated solely on MySpace's failure to implement basic safety measures to protect minors," to which the court responded:

Their claims are barred by the CDA, notwithstanding their assertion that they only seek to hold MySpace liable for its failure to implement measures that would have prevented Julie Doe from communicating with Solis.

Technically, the Doe case was a “failure-to-protect” case, not a “failure-to-warn” case, but it’s a distinction without a difference. Couldn’t Doe just as easily have sued MySpace for failing to warn her about the possibility of an offline sexual assault? It’s the same basic argument as her “failure to protect” claim.

Another even more directly relevant precedent was [Beckman v. Match.com](#), another offline assault facilitated by UGC publication tools. The court found Section 230 applicable because:

There is nothing for Match.com to negligently misrepresent or negligently fail to warn about other than what a user of the website may find on another user’s profile on the website.

The court didn’t discuss either Doe v. MySpace or the Beckman case. Why not? One possible reason is [Internet Brands’ breathtakingly short appellate brief](#) didn’t raise them (the Beckman case hadn’t been decided at the time, but it would have been a good subsequent supplement).

Finally, I would like to say a bit about the merits of the court’s Section 230 legal analysis. Section 230 doesn’t make a declarative statement about liability; it simply makes a declarative statement about “treatment as a publisher or speaker.” I understand the court’s thinking that a “failure to warn” claim never treats a UGC site as a publisher or speaker. Nevertheless, judicial interpretations of Section 230’s language over the past 2 decades make it clear that Section 230 applies when a UGC site exercises its editorial functions. The court makes the nails-on-chalkboard strawman assertion that “Congress has not provided an all purpose get-out-of-jail-free card for businesses that publish user content on the internet.” Duh—no one argued otherwise. Instead, the real question is whether the “failure to warn” claim is based on ModelMayhem’s exercise of editorial functions, and I think the answer is emphatically yes. Editorially publishing the plaintiff’s profile was the “but for” causation in this case; which (unlike the court’s strawman BS arguments) would not be the case for many other types of claims, such as wage-and-hour, income tax demands or failure to issue data breach notifications. So everyone agrees that Section 230 isn’t a categorical get-out-of-jail card, but when the underlying harm is allegedly caused by a UGC website publishing user content to a tortious/criminal actor, that’s clearly a Section 230 case as clarified by hundreds of precedent cases.

[Note: the Ninth Circuit’s [Riggs v. MySpace](#) case made it clear that the plaintiff’s own content can qualify as “information provided by another information content provider” for purposes of a Section 230 analysis.]

Related posts:

Blogspot Gets Section 230 Win In 11th Circuit–Dowbenko v. Google

Section 230 Applies to Amazon Book Reviews–Joseph v. Amazon

Section 230 Immunizes Website For Super-User’s Doxxing–Internet Brands v. Jape

Another Section 230 Win For Ripoff Report–Torati v. Hodak

Software Manufacturer Denied Section 230 Immunity–Hardin v. PDX

Facebook Gets Easy Section 230 Win in DC Circuit–Klayman v. Facebook

Linking to Defamatory Content Protected by Section 230 — Vazquez v. Buhl

Yelp Wins Another Section 230 Case–Kimzey v. Yelp

Ripoff Report’s Latest Section 230 Win–Seldon v. Magedson

Xcentric Ventures Chips Away at Small Justice’s Copyright Workaround to Section 230

Employer Gets Section 230 Immunity For Employee’s Posts–Miller v. FedEx

National Advertising Division (NAD) Doesn’t Consider Section 230 Defenses

WhitePages Gets Its Inevitable Section 230 Win–Nasser v. WhitePages

Section 230 Protects Another Newspaper From Liability For User Comments–Hupp v. Freedom Communications

YouTube Gets Easy Section 230 Win–Gavra v Google

Dentist’s Defamation Lawsuit Against Yelp Preempted by Section 230–Braverman v. Yelp

Talk Slides on Section 230, Anti-SLAPP Laws and Housing Anti-Discrimination

Gripping Blogger Protected by Fair Use But Not Section 230–Ascend Health v. Wells

Section 230 Still Keeping the Pro Se Plaintiffs at Bay–Klayman v. Facebook, and More

Section 230 Immunizes Links to Defamatory Third Party Content–Directory Assistants v. Supermedia

Yet Another Case Says Section 230 Immunizes Newspapers from User Comments–Hadley v. GateHouse Media

Angie’s List’s Telephone and Fax Information Services May Be Immunized by Section 230–Courtney v. Vereb

Section 230 Doesn’t Protect Employer From Negligent Supervision Claim–Lansing v. Southwest Airlines. Warning: Ugly Opinion

Backpage Gets TRO Against Washington Law Attempting to Bypass Section 230—Backpage v. McKenna

PissedConsumer Denied Section 230 Immunity and Can't Shake Extortion Claim—Vo v. Opinion Corp.

StubHub Gets Section 230 Immunity from Anti-Scalping Laws Because Users Set Prices—Hill v. StubHub

Roommates.com Isn't Dealing in Illegal Content, Even Though the Ninth Circuit Denied Section 230 Immunity Because It Was

Ninth Circuit Affirms Google's Section 230 Win Over a Negative Business Review—Black v. Google

Ninth Circuit Mucks Up 47 USC 230 Jurisprudence....AGAIN!?!—Barnes v. Yahoo

* * *

PRIVACY/SECURITY; PUBLICITY/PRIVACY RIGHTS

Sunbelt Rentals v. Victor, No. 13-4240-SBA (N.D. Cal. Aug. 28, 2014)

Employer Isn't Liable When Former Employee Linked His Apple Accounts To Its Devices

Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

Victor worked at Sunbelt as a sales rep but left to join a competitor. His former employer is suing him for trade secret misappropriation.

Victor asserted privacy-based counterclaims. Sunbelt assigned him an iPhone and an iPad. He created an Apple account linked to both devices. He returned the devices upon termination. He received an iPhone and iPad from his new employer, but when he went to link the iPad to his Apple account, he discovered that the previous phone was still linked to his account. As a result, his text messages were transmitted to the iPhone he returned to Sunbelt. He sued for violations of the Wiretap Act, Stored Communications Act and Section 502 of the California Penal Code.

His Wiretap Act claim fails because Victor could not allege that Sunbelt “intentionally” intercepted any messages. The court questions whether an “interception” occurred at all. Moreover, Victor’s actions (connecting the device to his account and later not un-linking the device) caused any interception that occurred.

His Stored Communications Act claims also fail. There's no allegation that Sunbelt accessed any of the messages. The court also questions whether texts on a phone are in "electronic storage" for purposes of the SCA.

Victor's statutory state law claims fail for similar reasons. As to his invasion of privacy tort claim, the court flatly rejects Victor's contention that he had a reasonable expectation of privacy in the communications generally. While it's possible that specific messages may carry a greater expectation of confidentiality, Victor did not make any supporting allegations about this. Even if he had some expectation of privacy, the court says he's out of luck:

The facts alleged demonstrate that he failed to comport himself in a manner consistent with objectively reasonable expectation of privacy. By his own admission, Victor personally caused the transmission of his text messages to the Sunbelt iPhone by syncing his new devices to his Apple account without first unlinking his Sunbelt iPhone. As such, even if he subjectively harbored an expectation of privacy in his text messages, such expectation cannot be characterized as objectively reasonable, since it was Victor's conduct that directly caused the transmission of his text messages to Sunbelt in the first instance.

For good measure, the court also says that even assuming an intrusion occurred, it falls short of anything that is highly offensive to the reasonable person.

This is an oddball factual scenario, but it's probably more common than one would expect. Employer investigations that delve into employee communications always seem somewhat risky (perhaps unavoidable). Although the claims here largely failed because Victor was the one who caused his texts to be forwarded, the variety of claims asserted highlight what legal tools are available to the terminated employee who asserts a privacy claim. (See [Pure Power](#); [Ehling](#).)

The case is somewhat analogous to the [Zaratzian case](#) in that privacy cases can turn on settings that determine who receives access or is forwarded messages. Both situations also involve life transitions (divorce, job change) and highlight the importance of reviewing automated settings during such transitions. It's important for the party who "owns" the account, but perhaps equally important for the party who receives forwarded messages as well.

Ultimately, a clear waiver by the employee would probably neutralize most of the claims. The waiver issue does not come up in this case, but I wonder how consent in this context would compare with consent in the email scanning cases.

Bonus question that also did not come up: would employee social media laws have any effect on this scenario? Unlikely, but the influence of the Apple account did bring this to mind. Given the ambiguous status of accounts, it would have been trivially easy for

the employer to violate this law. Would Sunbelt have violated the law by requesting that Victor take certain action with respect to the Apple account, to reveal details regarding what devices it was linked to, or perhaps have him de-link their device from account during the exit interview? We haven't seen much litigation of the social media password privacy statutes yet, but the voluminous number of drafting ambiguities in those statutes mean there is a high likelihood of disputes under those heading towards a litigation quagmire. (See Eric's post: "[The Spectacular Failure of Employee Social Media Privacy Laws](#)".)

related posts:

[When Is It Appropriate To Monitor An Ex-Spouse's Email Account? Never](#)

[Ex-Spouse Hit With 20K in Damages for Email Eavesdropping – Klumb v. Goan](#)

[Keylogger Software Company Not Liable for Eavesdropping by Ex-spouse — Hayes v. SpectorSoft](#)

[Ex-Employees Awarded \\$4,000 for Email Snooping by Employer — Pure Power Boot Camp v. Warrior Fitness Boot Camp](#)

[Court: Husband's Access of Wife's Email to Obtain Information for Divorce Proceeding is not Outrageous](#)

[Minnesota Appeals Court Says Tracking Statute Excludes Use of GPS to Track Jointly Owned Vehicle — State v. Hormann](#)

[NJ Appeals Court: No Privacy Violation When Spouse Uses GPS to Track Vehicle — Villanova v. Innovative Investigations, Inc.](#)

[Lawyer Who Advised Brother-in-Law Regarding the Use of Spyware on His Wife Disqualified in Ensuing Privacy Dispute — Zang v. Zang](#)

[Court Rejects Attempt to Hold Software Company Liable for Surveillance Conducted by Its Customer – Luis v. Zang](#)

* * *

California Tells Businesses: Stop Trying To Ban Consumer Reviews (Forbes Cross-Post)

Eric Goldman

<http://www.blog.ericgoldman.org>

© 2014 Professor Eric Goldman. Professor Goldman teaches at the University of Santa Clara Law School and is the Director of the school's High Tech Law Institute.

Increasingly, businesses are looking for ways to suppress or erase consumers' negative online reviews of them. In particular, we've recently seen a proliferation of contract clauses purporting to stop consumers from reviewing businesses online. Those overreaching contract clauses have never been a good idea, but last week, the idea got worse. Gov. Jerry Brown signed **AB 2365** into law, to be codified as California Civil Code Sec. 1670.8. The law is a first-in-the-nation statute to stop businesses from contractually gagging their consumers.

The **new law** says that a consumer contract "may not include a provision waiving the consumer's right to make any statement regarding the seller or lessor or its employees or agents, or concerning the goods or services." Any contract terms violating this provision are void. Simply including a prohibited clause in a contract, even if the business never enforces it, or threatening to enforce such a clause can lead to a penalty of up to \$2,500 (up to \$10,000 if the violation is willful). The penalties may be financially modest, but any California business foolish enough to take an anti-review contract to court will end up writing a check to their customers.

Instead of telling consumers they can't review the businesses, some businesses are imposing financial penalties on consumers for writing negative reviews. I **recently wrote about** a New York hotel's contract that fined customers \$500 if they, or their wedding guests, posted negative online reviews. Disputes over fines will rarely end up in court because the hotel simply deducted the fine from the customer's security deposit. Or other businesses, such as **KlearGear**, have filed negative credit reports against consumers who didn't pay the fine. A consumer could challenge the security deposit deduction or negative credit report in court, but few will.

The statute tries to address the fining tactic by saying it's unlawful to "penalize a consumer for making any statement protected under this section." The statute doesn't define what statements are "protected under this section," so I'm not sure how courts will interpret the provision. The **legislative history** expressly references the KlearGear situation, so I anticipate the statute will cover fines against customers for writing negative online reviews.

We've also seen businesses use intellectual property claims to inhibit or discourage consumer reviews. The most notorious was the scheme by Medical Justice that helped doctors get their patients to assign the copyright in unwritten reviews. Unfortunately, the statute doesn't directly address this situation, and arguably these IP-based tactics don't constitute "waivers" prohibited by the statute. Perhaps courts will nevertheless interpret the statute to ban these abusive practices; otherwise, I fear we'll see more IP-based anti-review shenanigans following this law.

If you're responsible for your business' contract with consumers, today's a good day to review the contract and confirm that you don't have any language that might be interpreted as a restriction on your customers' ability to review your business. There are **so many better ways** to handle consumer reviews.

[Note: the press coverage about the bill's passage has occasionally been confused because the legislature substantially amended it between introduction and passage and the coverage mistakenly addresses the initial bill version, not the bill as passed. Initially **the bill would have allowed consumers** to waive their review rights if the waiver were sufficiently well-informed; the final bill eliminates that option.]

* * *

PRIVACY/SECURITY

Zaratzian v. Abadir, 10 CV 9049 (VB) (S.D.N.Y. Sept 2, 2014)

When Is It Appropriate To Monitor An Ex-Spouse's Email Account? Never

Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

Zaratzian and Abadir were married but divorced after a little over a decade. While the couple was married, Abadir opened a Cablevision account for internet and email service. He configured an account for Zaratzian and set the password.

He also configured an account for himself. At some point before the couple's separation, Abadir configured the account to forward emails from Zaratzian's account to Abadir's account.

He testified that he activated the auto-forwarding function so to avoid missing notifications sent to Zaratzian about the kids' extracurricular activities; and he testified that Zaratzian agreed to this. (She disputed this.)

After the couple separated, Zaratzian took over the account. A few years later, she found out that Abadir's email account was still being maintained and she cancelled it. At

this point, she started receiving bouncebacks . . . of emails that were forwarded from her account to his account. She sued Abadir alleging violations of the Wiretap Act and the Stored Communications Act. (Her lawsuit was separate from the custody/dissolution proceeding.)

The court denies Abadir's motion for summary judgment, finding that even under a narrow interpretation of the term "intercept" Abadir's automatic forwarding of Zaratzian's email suffices (citing and discussing [Pure Power Boot Camp](#) and [US v. Szymuszekiwicz](#)):

The court agrees with the Sventh Circuit's commonsense application of the contemporaneity requirement in a case with materially identical facts. Here, too, whether it was the server of Zaratzian's computer that made copies that were transmitted to Abadir, those copies were made "within a second of each message's arrival and assembly," and if both Zaratzian and Abadir were at their computers in the same moment, they each would have received the message "with no more than an eyeblink in between."

Abadir argued consent. Citing Judge Koh's opinion in the [Gmail case](#) among others, the court says that implied consent is an "intensely factual question". (But see the Yahoo email scanning case for a different view.) Abadir argued Zaratzian never expressly revoked her consent, but the court says that the dispute is about the scope of the consent as originally given rather than whether she revoked it. Abadir also tried the ownership argument, saying he "owned" the email account at the time. The court rejects this argument and distinguishes Abadir's precedent on the basis that those cases involved (1) the Stored Communications Act (which has a separate exception) and (2) both involved professional email accounts:

Zaratzian had a reasonable expectation of privacy in her personal email, regardless of whether her husband's name was technically the name on the . . . account. To hold otherwise would lead to a perverse outcome in conflict with basic notions of privacy.

Zaratzian also sued Abadir's lawyer, saying that he knowingly disclosed information obtained in violation of the statute. The lawyer said there was no evidence that he knew of the underlying violations. The court agrees with this argument, noting that Zaratzian's anecdotal evidence that Abadir's lawyer must have knew of the interception is insufficient. Perhaps he knew the emails were improperly obtained, but the court says he has to know they were improperly intercepted.

Finally, Zaratzian also brought claims under the Stored Communications Act but she failed to respond to defendants' arguments as to those claims. She also argued that Abadir breached a fiduciary obligation to her that undermined the basis of their marital settlement, but she fails to show that any omission or misstatement materially altered the outcome of the settlement.

Yikes. PRO TIP: I presume the temptation is strong to monitor your soon-to-be-ex-spouse's email, but resist it at all costs! This is not the first time we've seen an ex-spouse into hot water, and I'm sure it won't be the last. (See, e.g., [Ex-Spouse Hit With 20K in Damages for Email Eavesdropping – Klumb v. Goan](#).) The ruling illustrates that ownership over the account in question or having your name on it is not a free pass. As in other cases, lawyers often become embroiled in these lawsuits, and here Abadir's lawyer was lucky to dodge a bullet.

I guess a corollary is to never share your email account with anyone. If you do, perhaps you should use some sort of mechanism to automatically revoke consent. The consent argument (or "ownership" for that matter) did not end up undermining Zaratzian's case but it would be nice to have clarity on this front. In the employment context for example, many separation agreements have a clause revoking any consent to previously authorized accounts. Perhaps there should be some similar protocol in the marriage/domestic partner context.

(For a bizarre set of facts around consent, see *Gridiron Management Group v. Pimmel*, where the defendant who accessed plaintiff's Yahoo account following termination of employment argued that plaintiff "gave [defendant] the password to his account [and] told [defendant] that he had nothing to hide and did not care who read his emails." Interestingly, even there the court found a factual dispute as to the scope of consent and denied plaintiff's motion for summary judgment. See also "[The Password Is Finally Dying. Here's Mine](#)".)

Other coverage: "[Wiretap Act Claim Proceeds After Man Gets Ex-Wife's Email](#)"

Related custody proceeding: *In re Annabelle Zaratzian* (April 24, 2013) [[pdf](#)]

Related posts:

[Ex-Spouse Hit With 20K in Damages for Email Eavesdropping – Klumb v. Goan](#)

[Keylogger Software Company Not Liable for Eavesdropping by Ex-spouse — Hayes v. SpectorSoft](#)

[Ex-Employees Awarded \\$4,000 for Email Snooping by Employer — Pure Power Boot Camp v. Warrior Fitness Boot Camp](#)

[Court: Husband's Access of Wife's Email to Obtain Information for Divorce Proceeding is not Outrageous](#)

[Minnesota Appeals Court Says Tracking Statute Excludes Use of GPS to Track Jointly Owned Vehicle — State v. Hormann](#)

NJ Appeals Court: No Privacy Violation When Spouse Uses GPS to Track Vehicle — Villanova v. Innovative Investigations, Inc.

Lawyer Who Advised Brother-in-Law Regarding the Use of Spyware on His Wife Disqualified in Ensuing Privacy Dispute — Zang v. Zang

Court Rejects Attempt to Hold Software Company Liable for Surveillance Conducted by Its Customer – Luis v. Zang

* * *

COPYRIGHT; LICENSING/ CONTRACTS

AFP v. Morel, 10-cv-2730 (AJN) (S.D.N.Y. Aug. 13, 2014)

Court Denies AFP/Getty Bid to Set Aside Morel Copyright Verdict

Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

The dust is settling on *AFP v. Morel*, and the wreckage that emerges isn't pretty.

Following trial, a jury awarded Morel \$1,503,889.77 in actual and statutory damages for infringement. The jury also found that defendants violated Morel's rights under the DMCA (by distributing false copyright management information or modifying/removing copyright management information) and awarded an additional \$20,000 for these violations. Defendants moved to set aside or reduce the verdict. The court largely denies the motion.

Willful Infringement: Both defendants argued there was insufficient evidence of willful infringement, so enhanced statutory damages were improper. The court says the evidence was "plainly sufficient" to support a jury finding that AFP acted willfully. The person at AFP who sourced the photos testified that he took at face value the statement of a person who claimed to have taken the photographs; and if he knew the person wasn't even in Haiti at the time, he would have questioned the authorization AFP purportedly received. Although he denied seeing tweets from the purported licensor indicating he was in the Dominican Republic and thus could have not have taken the photos, the jury was entitled to disbelieve him:

Amalvy testified that if he had seen Suero's tweets indicating that Suero was in the Dominican Republic, he would have questioned whether Suero had the right to authorize distribution of the photographs.

Although Amalvy said that he did not see these tweets, the jury could conclude from the fact that he sent multiple Twitter messages to Suero on the same night that he did, in fact see them.

Two other facts cut against AFP: (1) it did not cease distributing the photos immediately, perhaps believing that it could secure a retroactive license, and (2) it “works in an industry where copyright [is] prevalent and has . . . extensive experience with copyright ownership”.

The evidence as to Getty’s willfulness was thinner but also sufficient. Its culpability turned on whether it took corrective action after receiving a “kill notice” from AFP. Unfortunately, a day prior to issuing the kill notice, AFP issued a “caption correction” and this resulted in some confusion on Getty’s side about what images needed to be removed. Ultimately, it was Getty’s responsibility to remove the photos and any deficiency in notices from AFP did not absolve Getty. As with AFP, Getty also works in an industry where “copyright [is] prevalent”.

DMCA Liability: AFP’s caption corrections were sufficient to support a finding of liability under either section of the DMCA dealing with copyright management information. AFP added an identifier (AFP) to the images, and also changed the credit to Morel. When coupled with the fact that it knew the images were not properly licensed, the jury could reasonably find that AFP violated both subsections of the statute.

Getty’s DMCA argument suffers a similar fate—its continued distribution of improperly credited images satisfy section 1202(a). However, the court says there’s insufficient evidence for a finding of a 1202(b) violation. The court says that addition of identifiers does not equal “removal or alteration” of copyright management information and thus the addition of “AFP” and “Getty Images” doesn’t trigger 1202(b) liability. The evidence showed that the two ways information was removed or altered was (1) when Suero removed the image from Twitpic and (2) when AFP changed the photographer credit. There was no evidence that Getty knew or was a part of these underlying violations. With respect to the credit that was changed by AFP, although Getty continued to distribute Suero-credited images (which did not contain altered CMI) it did not continue to distribute Morel-credit images, which did contain the altered CMI. Thus, Getty is only half liable for the DMCA violations (and the awarded against it is reduced from \$20,000 to \$10,000).

Damages: Morel was awarded \$20,000 for 16 DMCA violations. Defendants argued that injury was distinct from a violation and Morel needed to show distinct injuries flowing from each violation. Defendants also argued that the DMCA damages overlapped with the copyright damages. The court rejects both arguments. Defendants also challenged the award for copyright infringement damages but this also falls on deaf ears. The court says

that there need not be “correlation” between actual and statutory damages. Even assuming some correlation is required, there was clearly demand for Morel’s images (indeed defendants licensed them):

The earthquake was a major news event, and there was evidence that pictures from on the ground were difficult to come by in its immediate aftermath. In other words, it would be reasonable to conclude that there would have been demand for Morel’s photographs had Defendants not made them widely available to their customers.

Defendants also argued that the amount of the verdict was “shocking to the conscience,” but this only happens in an extreme case and this is not such a case. (The court footnotes *Capitol Records v. Thomas-Rasset*.)

The obvious lesson to draw from this episode is that companies—particularly those who are selling copyrighted works or otherwise distributing them downstream—should not rely on permission granted via social media for copyrighted material. The evidence cited indicates a highly energized, harried environment for sourcing content in the aftermath of the catastrophe, but this was no reason to put aside AFP’s (and Getty’s) standard clearance procedures. It’s worth noting Eric’s comments from an earlier [blog post](#) on the case:

Despite the fact many people freely copy Internet photos, there are very few circumstances where republishing someone else’s photo without permission isn’t infringement, and the transaction costs of defending any such lawsuit almost always exceeds the upfront license fees.

The case also brings to mind the “stop digging” adage (the [First Law of Holes](#)). AFP inexplicably went scorched earth on Morel even though he clearly had a viable claim. Rather than settling with Morel, AFP dug in and continued to dig. It’s possible they truly believed that they had some license through Twitter’s or Twitpic’s terms of service but I’m skeptical. (See “[Court Definitely Rejects AFP’s Argument That Posting a Photo to Twitter Grants AFP a License to Freely Use It](#)“.) They’re still weighing their appeal options (they agreed to an extension of the deadline) but, as the fee petition filed by Morel’s former lawyer shows (she claims approximately \$750,000 for her efforts, which does not include trial), litigation costs alone will be in the \$3-4 million range. I would be shocked if Morel had been offered and turned down something approaching 50% of this number.

The court notes that both AFP and Getty work in an industry where copyright is “prevalent”. The court does not cite it directly, but AFP knows about copyright and can be litigious about it too. See [AFP v. Google](#). On a related note, recipients of Getty’s threat letters are probably allowed to enjoy a brief moment of Schadenfreude.

A final thought is that the case raised some interesting issues relating to copyright management information and DMCA claims generally. Given that the DMCA award is only a tiny portion of the overall damage award, I would be surprised if the DMCA issue ends up figuring prominently or even being mentioned on appeal.

A tangentially related recent bit of news: “[Photo App Twitpic Shuts Down Over Trademark Spat With Twitter](#)”.

Related posts:

[AFP & Getty’s Republication of Twitter/Twitpic-Sourced Photos Turns Out to Be Costly – AFP v. Morel](#)

[AFP v. Morel – Lawsuit Over Haiti Photos Taken From Twitter/Twitpic Goes to Trial](#)

[Court Definitively Rejects AFP’s Argument That Posting a Photo to Twitter Grants AFP a License to Freely Use It — AFP v. Morel](#)

[Court Rejects Agence France-Presse’s Attempt to Claim License to Haiti Earthquake Photos Through Twitter/Twitpic Terms of Service — AFP v. Morel](#)

[Agence France-Presse Claims Twitter’s Terms of Use Authorize Its Use of Photographs Posted to TwitPic — Agence France-Presse v. Morel](#)

* * *

E-COMMERCE; MARKETING

Imber-Gluck v. Google, 14-cv-1070 (N.D. Cal. July 21, 2014)

Lawsuit Against Google Over In-App Purchases By Minors Squeaks Past Motion to Dismiss

Venkat Balasubramani

© 2014 Venkat Balasubramani. Venkat Balasubramani is a principal at Focal PLLC.

This is a lawsuit against Google over in-app purchases made by minor children, reminiscent of a similar lawsuit against Apple. Plaintiff on behalf of a putative class alleged that, among other things, Google allowed someone to make a purchase for thirty minutes (as opposed to Apple’s 15 minute window) after entering their account information and this meant her children racked up purchases.

Disaffirmance/contracts with minors: Contracts with minors can be disaffirmed, but the minor has to be the one who disaffirms the agreement. Here, plaintiff didn’t bring claims

on behalf of her child, so she doesn't have standing to disaffirm. Google makes a separate argument that the terms of service control all purchases made through the platform, and the terms say that account-holders are responsible for transactions conducted through their account (i.e., responsible for making sure no one misuses their password). Plaintiff tries to argue that the terms are ambiguous, but the court disagrees.

The court dismisses both of these claims.

Consumer Legal Remedies Act Claim: Plaintiff argued that Google failed to disclose material facts about the apps – namely, that although they were advertised as free (or at nominal cost), they could be used to make further purchases. The court also dismisses this claim, saying that while plaintiff adequately alleged a possibly misleading statement, or withholding of a material fact, she did not allege reliance.

Unfair Competition Claims: Of the various types of unfair competition claims, the court says that only her claim under the “unfair, deceptive or misleading” prong is adequate. The court liked plaintiff's allegation that:

Google actively advertised, marketed and promoted certain gaming Apps as “free” with the intent to lure minors to purchase Game Currency in a manner likely to deceive the public.

The court declines to dismiss this claim.

Unjust enrichment: The parties argue over whether this is a standalone cause of action or a remedy. The court says, citing to the Apple in-app purchase case among others, that it will allow plaintiff's to proceed with it at this stage.

Duty of Good Faith: The court allows this claim to go forward as well. Google argued that an implied duty of good faith can't be used to contradict a specific term of the agreement (that account-holders are responsible for their activity) but the court disagrees. The provision regarding authorized charges merely allows Google to bill the account-holder, but plaintiff's allegation that Google encouraged children to make in-app purchases is separate from this term.

This looks like a similar result to the Apple in-app purchase case. Apple settled that lawsuit and separately settled with the FTC as well. “[Apple to Refund App Store Purchases Made Without Parental Consent.](#)”

Normally, e-commerce companies don't get bogged down in litigation over their practices, and it's tough to pinpoint exactly what's different here, other than perhaps the transactions involve minors. The [C.M.D. v. Facebook](#) case provided some clarity to contracting with minors (and allowed prospective disaffirmance), but a distinguishing fact here is the involvement of virtual goods. I'm not exactly sure how disaffirmance, if

properly implemented, would play out here. Would you have to agree to deletion of the virtual good? But the cases end up hinging on a vague idea of a misleading practice, even though there's very little fleshed out about what is misleading in the advertising and what statements are made by Google versus by the app developer. Maybe courts and plaintiffs think the platforms should take affirmative steps to prevent purchases, or give parents the option of additional controls? (See, e.g., "[Morally Responsible Apps Are The Need Of The Hour](#)".) For what it's worth, in the FTC's action against Apple, Commissioner Wright issued a dissenting statement that asked whether it made sense for the FTC to crack down on Apple in-app purchases: "Dissenting Statement of Commissioner Joshua D. Wright; In the Matter of Apple, Inc." [[pdf](#)].

[Note: between the ruling and blog post, Plaintiff filed an amended complaint.]

Related posts:

[Parents' Lawsuit Against Apple for In-App Purchases by Minor Children Moves Forward — In re Apple In-App Purchase Litigation](#)

[Court Rules That Kids Can Be Bound By Facebook's Member Agreement](#)

[Minors' Suit Over Facebook Credits Continues — I.B. v. Facebook](#)

[Minors' Suit Over Facebook Credits Survives in Part — I.B. v. Facebook](#)

* * *

FOR PUBLICATION

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

JOSE GOMEZ, individually and on
behalf of a class of similarly situated
individuals,

Plaintiff-Appellant,

v.

CAMPBELL-EWALD COMPANY,

Defendant-Appellee.

No. 13-55486

D.C. No.
2:10-cv-02007-
DMG-CW

OPINION

Appeal from the United States District Court
for the Central District of California
Dolly M. Gee, District Judge, Presiding

Argued and Submitted
July 11, 2014—Pasadena, California

Filed September 19, 2014

Before: Fortunato P. Benavides,* Kim McLane Wardlaw,
and Richard R. Clifton, Circuit Judges.

Opinion by Judge Benavides

* The Honorable Fortunato P. Benavides, Senior Circuit Judge for the
U.S. Court of Appeals for the Fifth Circuit, sitting by designation.

SUMMARY**

Telephone Consumer Protection Act

The panel vacated the district court's summary judgment in favor of the defendant on personal and putative class claims under the Telephone Consumer Protection Act.

The plaintiff alleged that the defendant company instructed or allowed a third-party vendor to send unsolicited text messages on behalf of the United States Navy, with which the defendant had a marketing contract.

The panel held that pursuant to *Diaz v. First Am. Home Buyers Prot. Corp.*, 732 F.3d 948 (9th Cir. 2013), the plaintiff's individual claim was not mooted by his refusal to accept a settlement offer under Federal Rule of Civil Procedure 68. Pursuant to *Pitts v. Terrible Herbst, Inc.*, 653 F.3d 1081 (9th Cir. 2011), the putative class claims were not mooted where the plaintiff rejected the settlement offer before he moved for class certification. The panel concluded that *Pitts* and *Diaz* were not clearly irreconcilable with *Genesis Healthcare Corp. v. Symczyk*, 133 S. Ct. 1523 (2013) (addressing collective action brought pursuant to Fair Labor Standards Act).

The panel held that 47 U.S.C. § 227(b)(1)(A)(iii), which restricts unsolicited text messaging, does not violate the First Amendment.

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The panel held that a defendant may be held vicariously liable for TCPA violations where the plaintiff establishes an agency relationship, as defined by federal common law, between the defendant and a third-party caller.

Finally, the panel held that the defendant was not entitled to derivative sovereign immunity. It remanded the case for further proceedings consistent with this opinion.

COUNSEL

Evan M. Meyers (argued), McGuire Law, P.C., Chicago, Illinois; Michael J. McMorrow, McMorrow Law, P.C., Chicago, Illinois; and David C. Parisi, Parisi & Havens LLP, Sherman Oaks, California, for Plaintiff-Appellant.

Laura A. Wytsma (argued), Michael L. Mallow, Christine M. Reilly, and Meredith J. Siller, Loeb & Loeb LLP, Los Angeles, California, for Defendant-Appellee.

OPINION

BENAVIDES, Circuit Judge:

Plaintiff Jose Gomez appeals adverse summary judgment on personal and putative class claims brought pursuant to the Telephone Consumer Protection Act (“TCPA”), 47 U.S.C. § 227(b)(1)(A)(iii) (2012). Gomez alleges that the Campbell-Ewald Company instructed or allowed a third-party vendor to send unsolicited text messages on behalf of the United States Navy, with whom Campbell-Ewald had a marketing contract.

Because we conclude that Campbell-Ewald is not entitled to immunity, and because we find no alternate basis upon which to grant its motion for summary judgment, we vacate the judgment and remand to the district court.

I.

The facts with respect to Gomez’s personal claim are largely undisputed. On May 11, 2006, Gomez received an unsolicited text message stating:

Destined for something big? Do it in the Navy. Get a career. An education. And a chance to serve a greater cause. For a FREE Navy video call [number].

The message was the result of collaboration between the Navy and the Campbell-Ewald Company,¹ a marketing consultant hired by the Navy to develop and execute a multimedia recruiting campaign. The Navy and Campbell-Ewald agreed to “target” young adults aged 18 to 24, and to send messages only to cellular users that had consented to solicitation. The message itself was sent by Mindmatics, to whom the dialing had been outsourced. Mindmatics was responsible for generating a list of phone numbers that fit the stated conditions, and for physically transmitting the messages. Neither the Navy nor Mindmatics is party to this suit.

In 2010, Gomez filed the present action against Campbell-Ewald, alleging a single violation of 47 U.S.C. § 227(b)(1)(A)(iii), which states:

¹ The company is now known as Lowe Campbell Ewald.

It shall be unlawful for any person within the United States, or any person outside the United States if the recipient is within the United States—

(A) to make any call (other than a call made for emergency purposes or made with the prior express consent of the called party) using any automatic telephone dialing system or an artificial or prerecorded voice— . . .

(iii) to any telephone number assigned to a paging service [or] cellular telephone service

Gomez contends that he did not consent to receipt of the text message. He also notes that he was 40 years old at the time he received the message, well outside of the Navy's target market. It is undisputed that a text message constitutes a call for the purposes of this section. *See Satterfield v. Simon & Schuster, Inc.*, 569 F.3d 946, 952 (9th Cir. 2009) (“[W]e hold that a text message is a ‘call’ within the meaning of the TCPA.”). In addition to seeking compensation for the alleged violation of the TCPA, Gomez also sought to represent a putative class of other unconsenting recipients of the Navy's recruiting text messages.

After a 12(b)(6) motion to dismiss was denied, Campbell-Ewald tried to settle the case. Campbell-Ewald offered Gomez \$1503.00 per violation, plus reasonable costs, but Gomez rejected the offer by allowing it to lapse in accordance with its own terms.

Campbell-Ewald then moved to dismiss the case under Rule 12(b)(1), arguing that Gomez’s rejection of the offer mooted the personal and putative class claims. After the court denied the motion, Campbell-Ewald moved for summary judgment, seeking derivative immunity under *Yearsley v. W.A. Ross Construction Co.*, 309 U.S. 18 (1940). In opposition to the summary judgment motion, Gomez presented evidence that the Navy intended the messages to be sent only to individuals who had consented or “opted in” to receive messages like the recruiting text. A Navy representative testified that Campbell-Ewald was not authorized to send texts to individuals who had not opted in. The district court ultimately granted the motion, holding that Campbell-Ewald is “immune from liability under the doctrine of derivative sovereign immunity.” *Gomez v. Campbell-Ewald Co.*, No. CV 10-2007 DMG CWX, 2013 WL 655237, at *6 (C.D. Cal. Feb. 22, 2013). Gomez filed a timely appeal, arguing that the *Yearsley* doctrine is inapplicable.

This Court reviews summary judgment *de novo*, affirming only where there exists no genuine dispute of material fact. *Satterfield*, 569 F.3d at 950; *see also* FED. R. CIV. P. 56(a). We are free to affirm “on any basis supported by the record.” *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040, 1047 (9th Cir. 2009).

II.

We begin with jurisdiction. Upon Gomez’s timely appeal, Campbell-Ewald filed a motion to dismiss for lack of jurisdiction, arguing that the personal and putative class claims were mooted by Gomez’s refusal to accept the settlement offer. We denied that motion without prejudice, and now reject Campbell-Ewald’s argument on the merits.

Gomez’s individual claim is not moot. Campbell-Ewald argues that “whether or not the class action here is moot,” the individual claim was mooted by Gomez’s rejection of the offer. The company is mistaken. Although this issue was unsettled until recently, we have now expressly resolved the question. “[A]n unaccepted Rule 68 offer that would fully satisfy a plaintiff’s claim is insufficient to render the claim moot.” *Diaz v. First Am. Home Buyers Prot. Corp.*, 732 F.3d 948, 950 (9th Cir. 2013). Because the unaccepted offer alone is “insufficient” to moot Gomez’s claim, and as Campbell-Ewald identifies no alternate or additional basis for mootness, the claim is still a live controversy.

Similarly, the putative class claims are not moot. We have already explained that “an unaccepted Rule 68 offer of judgment—for the full amount of the named plaintiff’s individual claim and made before the named plaintiff files a motion for class certification—does not moot a class action.” *Pitts v. Terrible Herbst, Inc.*, 653 F.3d 1081, 1091–92 (9th Cir. 2011). Like the *Pitts* plaintiff, Gomez rejected the offer before he moved for class certification. Gomez’s rejection therefore does not affect any class claims.

Campbell-Ewald recognizes that it is asking this panel to depart from these precedents. Yet it is well settled that we are bound by our prior decisions. *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). Although there is an exception for precedents that have been overruled, that exception applies only where “the relevant court of last resort [has] undercut the theory or reasoning underlying the prior circuit precedent in such a way that the cases are clearly irreconcilable.” *Ibid.* Campbell-Ewald argues that *Pitts* and *Diaz* are clearly irreconcilable with the Supreme Court’s recent decision in *Genesis Healthcare Corp. v. Symczyk*, —

U.S. —, 133 S. Ct. 1523 (2013). Campbell-Ewald overstates the relevance of that case, which involved a collective action brought pursuant to § 16(b) of the Fair Labor Standards Act. *Id.* at 1526–27. The defendant argued that the case was mooted by the plaintiff’s rejection of a settlement offer of complete relief. *Id.* at 1528. The Supreme Court ultimately agreed, first accepting the lower court’s conclusion that the personal claim was moot, and then holding that the named plaintiff had “no personal interest in representing putative, unnamed claimants, nor any other continuing interest that would preserve her suit from mootness.” *Id.* at 1532.

Campbell-Ewald correctly observes that *Genesis* undermined some of the reasoning employed in *Pitts* and *Diaz*. For example, the *Pitts* opinion referred to the risk that a defendant might “pick off” named plaintiffs in order to evade class litigation. 653 F.3d at 1091 (quoting *Weiss v. Regal Collections*, 385 F.3d 337, 344 (3d Cir. 2004)). The *Genesis* Court distanced itself from such reasoning, pointing out that the argument had only been used once by the high Court, and only “in dicta.” 133 S. Ct. at 1532 (referring to *Deposit Guar. Nat’l Bank, Jackson, Miss. v. Roper*, 445 U.S. 326, 339 (1980)). Nevertheless, courts have universally concluded that the *Genesis* discussion does not apply to class actions.² In fact, *Genesis* itself emphasizes that “Rule 23

² At least ten courts had expressly stated that the *Genesis* analysis does not bind courts with respect to class action claims. *E.g.*, *Epstein v. JPMorgan Chase & Co.*, No. 13 Civ. 4744(KPF), 2014 WL 1133567, at *9 (S.D.N.Y. Mar. 21, 2014) (“The court agrees with Plaintiff that these [prior class action] cases were not affected by the Supreme Court’s recent decision in *Genesis*”); *Knutson v. Schwan’s Home Serv., Inc.*, No. 3:12-cv-0964-GPC-DHB, 2013 WL 4774763, at *11 (S.D. Cal. Sept. 5, 2013) (concluding that *Pitts* was not affected by *Genesis*). We are not aware of any court that has held otherwise.

[class] actions are fundamentally different from collective actions under the FLSA” and, therefore, the precedents established for one set of cases are “inapplicable” to the other. 133 S. Ct. at 1529. Accordingly, because *Genesis* is not “clearly irreconcilable” with *Pitts* or *Diaz*, this panel remains bound by circuit precedent, and Campbell-Ewald’s mootness arguments must be rejected. *Miller*, 335 F.3d at 900.

III.

Campbell-Ewald’s constitutional challenge is equally unavailing. The company argues that the statute is unconstitutional either facially or as applied, but its argument relies upon a flawed application of First Amendment principles. Although the district court did not ultimately reach this issue, the record confirms that the challenge was properly raised below.

We have already affirmed the constitutionality of this section of the TCPA. *Moser v. FCC*, 46 F.3d 970, 973–74 (9th Cir. 1995). The government may impose reasonable restrictions on the time, place, or manner of protected speech, provided that the restrictions “are justified without reference to the content of the restricted speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information.” *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (quoting *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984) (other citations omitted)). In analyzing the section, the *Moser* Court focused on the content-neutral statutory language. “Because nothing in the statute requires the [Federal Communications Commission] to distinguish between commercial and

noncommercial speech, we conclude that the statute should be analyzed as a content-neutral time, place, and manner restriction.”³ We then upheld the statute after finding that the protection of privacy is a significant interest, the restriction of automated calling is narrowly tailored to further that interest, and the law allows for “many alternative channels of communication.” *Id.* at 974–75.

Campbell-Ewald does not contest our reasoning in *Moser*. Instead, Campbell-Ewald argues that the government’s interest only extends to the protection of residential privacy, and that therefore the statute is not narrowly tailored to the extent that it applies to cellular text messages. The argument fails. First, this Court already applies the TCPA to text messages. *Satterfield*, 569 F.3d at 951–52. Second, there is no evidence that the government’s interest in privacy ends at home—the fact that the statute reaches fax machines suggests otherwise. *See* 47 U.S.C. § 227(b)(1)(C). Third, to whatever extent the government’s significant interest lies exclusively in residential privacy, the nature of cell phones renders the restriction of unsolicited text messaging all the more necessary to ensure that privacy. After all, it seems safe to assume that most cellular users have their phones with them when they are at home. Campbell-Ewald itself notes that in many households a cell phone *is* the home phone. In fact, recent statistics suggest that over 40% of American households now rely exclusively on wireless telephone

³ 46 F.3d at 973. Campbell-Ewald does not argue that the statute is no longer content neutral insofar as some implementing regulations distinguish between commercial and noncommercial calls. *See* 47 C.F.R. § 64.1200(a)(2) (2014); *cf. Destination Ventures, Ltd. v. FCC*, 46 F.3d 54, 56 (9th Cir. 1995) (holding that the TCPA’s treatment of commercial facsimile transmissions, 42 U.S.C. § 227(b)(1)(C), is a constitutionally permitted content-based restriction).

service.⁴ As a consequence, prohibiting automated calls to land lines alone would not adequately safeguard the stipulated interest in residential privacy. For all these reasons, Campbell-Ewald's argument is without merit.

Nor does the government speech doctrine provide Campbell-Ewald with a meritorious constitutional challenge. Campbell-Ewald argues that military recruiting messages are a form of government speech afforded greater protection by the First Amendment. Campbell-Ewald mischaracterizes the doctrine. The government speech doctrine is a jurisprudential theory by which the federal government can regulate its own communication "without the constraint of viewpoint neutrality." *Downs v. L.A. Unified Sch. Dist.*, 228 F.3d 1003, 1017 (9th Cir. 2000), *cert. denied*, 532 U.S. 994 (2001). For example, the First Amendment does not require the federal government to fund messages both for and against abortion. *Cf. Rust v. Sullivan*, 500 U.S. 173, 203 (1991) (upholding, under the government speech doctrine, regulations forbidding certain publicly funded doctors from endorsing abortion). Similarly, in this context, the doctrine would preclude Campbell-Ewald from demanding that the Navy create an advertising campaign that discourages military participation. The government speech doctrine is simply immaterial to the present dispute, in which the plaintiff is not advocating for viewpoint neutrality, but is instead challenging the regulation of a particular means of communication.

⁴ See Karen Kaplan, *Still have a land line? 128 million don't.*, L.A. TIMES, July 8, 2014, <http://www.latimes.com/science/sciencenow/la-sci-sn-wireless-only-households-in-america-20140708-story.html>.

IV.

Campbell-Ewald nevertheless argues that it cannot be held liable for TCPA violations because it outsourced the dialing and did not actually make any calls on behalf of its client. *See* 47 U.S.C. § 227(b)(1)(A)(iii) (rendering it unlawful “to make any call” using an automated dialing system). Gomez, in fact, concedes that a third party transmitted the disputed messages. Even so, Campbell-Ewald’s argument is not persuasive.

Although Campbell-Ewald did not send any text messages, it might be vicariously liable for the messages sent by Mindmatics. The statute itself is silent as to vicarious liability. We therefore assume that Congress intended to incorporate “ordinary tort-related vicarious liability rules.” *Meyer v. Holley*, 537 U.S. 280, 285 (2003). Accordingly, “[a]bsent a clear expression of Congressional intent to apply another standard, the Court must presume that Congress intended to apply the traditional standards of vicarious liability” *Thomas v. Taco Bell Corp.*, 879 F. Supp. 2d 1079, 1084 (C.D. Cal. 2012), *aff’d*, — F. App’x —, 2014 WL 2959160 (9th Cir. July 2, 2014) (per curiam). Although we have never expressly reached this question, several of our district courts have already concluded that the TCPA imposes vicarious liability where an agency relationship, as defined by federal common law, is established between the defendant and a third-party caller.⁵

⁵ *Ibid.* *See also* *Kristensen v. Credit Payment Servs.*, No. 2:12–CV–00528–APG, — F. Supp. 2d —, 2014 WL 1256035 (D. Nev. Mar. 26, 2014); *In re Jiffy Lube Int’l Inc.*, 847 F. Supp. 2d 1253 (S.D. Cal. 2012); *Kramer v. Autobytel, Inc.*, 759 F. Supp. 2d 1165 (N.D. Cal. 2010).

This interpretation is consistent with that of the statute's implementing agency, which has repeatedly acknowledged the existence of vicarious liability under the TCPA. The Federal Communications Commission is expressly imbued with authority to "prescribe regulations to implement the requirements" of the TCPA. 47 U.S.C. § 227(b)(2). As early as 1995, the FCC stated that "[c]alls placed by an agent of the telemarketer are treated as if the telemarketer itself placed the call." *In re Rules and Regulations Implementing the TCPA of 1991*, 10 FCC Rcd. 12391, 12397 (1995). More recently, the FCC has clarified that vicarious liability is imposed "under federal common law principles of agency for violations of either section 227(b) or section 227(c) that are committed by third-party telemarketers." *In re Joint Petition Filed by Dish Network, LLC*, 28 FCC Rcd. 6574, 6574 (2013). Because Congress has not spoken directly to this issue and because the FCC's interpretation was included in a fully adjudicated declaratory ruling, the interpretation must be afforded *Chevron* deference. *Metrophones Telecomms., Inc. v. Global Crossing Telecomms, Inc.*, 423 F.3d 1056, 1065 (9th Cir. 2005) (citing *Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs.*, 545 U.S. 967, 980–85 (2005)) (other citations omitted), *aff'd*, 550 U.S. 45 (2007); *see also Chevron, U.S.A., Inc. v. Natural Res. Def. Council*, 467 U.S. 837, 843 (1984) ("If, however, the court determines Congress has not directly addressed the precise question at issue, the court does not simply impose its own construction on the statute, as would be necessary in the absence of an administrative interpretation." (footnote omitted)).

Campbell-Ewald concedes that the FCC already recognizes vicarious liability in this context, but argues that vicarious liability only extends to the merchant whose goods or services are being promoted by the telemarketing

campaign. Yet the statutory language suggests otherwise, as § 227(b) simply imposes liability upon “any person”—not “any merchant.” See *Ali v. Fed. Bureau of Prisons*, 552 U.S. 214, 221 (2008) (interpreting the use of “any” as “all-encompassing”); 47 C.F.R. § 64.1200 (interpreting the phrase “any person” to reach individuals and entities). And although the FCC’s 2013 ruling may emphasize vicarious liability on the part of merchants, the FCC has never stated that vicarious liability is *only* applicable to these entities.⁶ Indeed, such a construction would contradict “ordinary” rules of vicarious liability, *Meyer*, 537 U.S. at 285, which require courts to consider the interaction between the parties rather than their respective identities. See RESTATEMENT (THIRD) OF AGENCY (2006) §§ 2.01, 2.03, 4.01 (explaining that agency may be established by express authorization, implicit authorization, or ratification).

Given Campbell-Ewald’s concession that a merchant can be held liable for outsourced telemarketing, it is unclear why a third-party marketing consultant shouldn’t be subject to that same liability. As a matter of policy it seems more important to subject the consultant to the consequences of TCPA infraction. After all, a merchant presumably hires a consultant in part due to its expertise in marketing norms. It

⁶ *Dish Network*, 28 FCC Rcd. at 6574. The FCC uses the word “seller,” which Campbell-Ewald construes as the merchant whose goods or services are featured in the telemarketing campaign. The FCC actually defines seller as an “entity on whose behalf a telephone call or message is initiated for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services.” See 47 C.F.R. § 64.1200(f)(9). We need not determine whether Campbell-Ewald constitutes a seller under this definition, as we conclude that vicarious liability turns on the satisfaction of relevant standards of agency, irrespective of a defendant’s nominal designation.

makes little sense to hold the merchant vicariously liable for a campaign he entrusts to an advertising professional, unless that professional is equally accountable for any resulting TCPA violation. In fact, Campbell-Ewald identifies no case in which a defendant was exempt from liability due to the outsourced transmission of the prohibited calls.

Moreover, our own precedent belies any argument that liability is not possible. In our seminal case regarding text messages and the TCPA, we allowed a case to proceed against an analogous marketing consultant who was not “responsible for the actual transmission of the text messages.” See *Satterfield*, 569 F.3d at 951. In *Satterfield*, a publisher had instructed a marketing consultant to create a text message campaign advertising a new Stephen King novel. *Id.* at 949. The consultant in turn outsourced the recipient selection and message transmission to two other subcontractors. *Id.* A recipient sued both the publisher and the marketing consultant for alleged violations of the TCPA. *Id.* at 950. The district court entered summary judgment in favor of both defendants, holding that the cellular user had consented to receive advertisements when it signed its cellular service contract. *Id.* We ultimately reversed and remanded the case, holding (*inter alia*) that the cellular service agreement did not constitute “express consent” to receive the advertisement in dispute. *Id.* at 955. So although we did not explain the basis of the defendants’ potential liability, we implicitly acknowledged the existence of that basis. The present case affords an opportunity to clarify that a defendant may be held vicariously liable for TCPA violations where the plaintiff establishes an agency relationship, as defined by federal common law, between the defendant and a third-party caller.

Before moving on, we should note that Gomez asks us to endorse another potential source of liability by holding that direct liability applies where a third party is “closely involved” in the placing of the calls. Because the facts are not yet developed, the present case does not require such a determination. We therefore leave that question for another day. *See United States v. Manning*, 527 F.3d 828, 837 n.8 (9th Cir. 2008) (“[W]e simply express no view on issues unnecessary to this [decision].” (citation omitted)).

V.

Finally, we turn to the legal theory underlying the district court’s decision. The court entered summary judgment after concluding that Campbell-Ewald is exempt from liability under *Yearsley*, 309 U.S. 18. Gomez contends that *Yearsley* is outdated and inapposite, and that the district court should have applied the standard articulated in *Boyle v. United Technologies Corp.*, 487 U.S. 500 (1988). The availability of these defenses is a question of law that we review *de novo*. *In re Hanford Nuclear Reservation Litig.*, 534 F.3d 986, 1000 (9th Cir. 2008).

After reviewing the relevant law, we agree with Gomez that *Yearsley* is not applicable. *Yearsley* established a narrow rule regarding claims arising out of property damage caused by public works projects. The dispute involved erosion caused by efforts to render the Missouri River more navigable. *Yearsley*, 309 U.S. at 19. The Court reasoned that if—as alleged—the contractor’s work was in accordance with express Congressional directive and resulted in an unconstitutional taking of property, “the Government has impliedly promised to compensate the plaintiffs and has afforded a remedy for its recovery by a suit in the Court of

Claims.” *Id.* at 21–22 (citing 28 U.S.C. § 250 (1940)) (other citations omitted). As a consequence, there was an adequate remedy available and no need for action against the private contractor. *Id.* at 22.

It seems clear that the reasoning employed by the *Yearsley* Court is not relevant here. Gomez’s claims do not implicate a constitutional “promise to compensate” injured plaintiffs such that an alternate remedy exists. Nor does the case belong in some other venue. *Cf. Myers v. United States*, 323 F.2d 580, 583 (9th Cir. 1963) (remanding under *Yearsley* for transfer to Court of Claims). Instead, Congress has expressly created a federal cause of action affording individuals like Gomez standing to seek compensation for violations of the TCPA. In the seventy-year history of the *Yearsley* doctrine, it has apparently never been invoked to preclude litigation of a dispute like the one before us. This Court, in particular, has rarely allowed use of the defense, and only in the context of property damage resulting from public works projects.

In its brief discussion, the district court did not explain its decision to apply *Yearsley* to the facts and issues at bar. The cases cited by the court do not support such an interpretation.⁷ At oral argument, we asked Campbell-Ewald to name any authority that might justify the application of *Yearsley* to the facts of this case. Campbell-Ewald responded by pointing to a recent Fifth Circuit decision dismissing a class action under

⁷ See *Ackerson v. Bean Dredging LLC*, 589 F.3d 196, 204–07 (5th Cir. 2009) (applying *Yearsley* in traditional public works context); *Butters v. Vance Int’l Inc.*, 225 F.3d 462, 466 (4th Cir. 2000) (adjudicating immunity under the Foreign Sovereign Immunity Act); *Myers*, 323 F.2d at 583 (applying *Yearsley* to property loss resulting from highway construction).

Yearsley. See *Ackerson*, 589 F.3d 196. Yet that case—like *Yearsley* itself—involved allegations of property damage resulting from dredging work undertaken to improve the nation’s waterways. *Id.* at 202–03 (listing allegations that the United States and its contractors had irreparably damaged Louisiana’s coastline and wetlands in the 1960s, ultimately contributing to the widespread loss of property during Hurricane Katrina). So while the Fifth Circuit’s decision may rebut Gomez’s argument that *Yearsley* is stale precedent, it does not warrant application of the doctrine to the present dispute.

Nor does the *Boyle* pre-emption doctrine provide Campbell-Ewald with a relevant defense. The doctrine precludes state claims where the imposition of liability would undermine or frustrate federal interests. See *Nielsen v. George Diamond Vogel Paint Co.*, 892 F.2d 1450, 1454 (9th Cir. 1990) (explaining that the *Boyle* standard is used to determine when “federal law should displace state law”). *Boyle* involved a wrongful death action brought under Virginia law against a government contractor that had supplied a helicopter to the United States military. See 487 U.S. at 502. After a jury returned a verdict in favor of the plaintiffs, the Fourth Circuit reversed, holding that liability was precluded in part by the federal interest inherent in military decisions. *Id.* at 503, 510. The Supreme Court agreed, explaining that when “an area of uniquely federal interest” is implicated by a federal purchase, state law is displaced where “a significant conflict exists between an identifiable federal policy or interest and the operation of state law, or the application of state law would frustrate specific objectives of federal legislation” *Id.* at 507 (internal brackets, quotation marks, and citations omitted). The Court then remanded after establishing a rule by which

courts should determine whether a specific contractor is acting pursuant to a military contract such that the defense is available. *Id.* at 512.

Although *Boyle* in effect created a defense for some government contractors, it is fundamentally a pre-emption case. The *Boyle* Court established two related rules: (1) a general rule whereby state claims may be pre-empted by federal law, and (2) a specific rule whereby certain military contractors may be exempt from state tort liability in furtherance of that pre-emption. 487 U.S. at 507–08, 512. In arguing that *Boyle* governs here, Gomez overlooks the pre-emption predicate, assuming that *Boyle* represents a general grant of immunity for government contractors. Yet *Boyle* itself includes footnotes emphasizing the displacement question and indicating that it should not be construed as broad immunity precedent. *Id.* at 505 n.1, 508 n.3. We have already clarified this point, explaining that *Boyle* “is directed toward deciding the extent to which federal law should displace state law with respect to the liability of a military contractor.” *Nielsen*, 892 F.2d at 1454. Accordingly, although *Boyle* may apply more broadly than to the facts of that case alone, that broader applicability is rooted in pre-emption principles and not in any widely available immunity or defense.

Returning to the present case, Gomez brings a claim under federal law, so pre-emption is simply not an issue. The *Boyle* doctrine is thus rendered inapposite. Even Campbell-Ewald—notwithstanding a vested interest in maintaining every possible means of exoneration—admits that a *Boyle* defense is not permissible here. Because the defendant does not assert a *Boyle* defense, we need not belabor the present

discussion—we accept Campbell-Ewald’s concession that *Boyle* is not relevant.

Campbell-Ewald contends that a new immunity for service contractors was espoused by the Supreme Court in *Filarsky v. Delia*, — U.S. —, 132 S. Ct. 1657 (2012). Yet the Court did not establish any new theory, and although the *Filarsky* discussion does include a broad reading of the qualified immunity doctrine, *id.* at 1667–68, that doctrine is not implicated by this case. *Filarsky* involved alleged constitutional violations brought pursuant to 42 U.S.C. § 1983. *See id.* at 1661. The Supreme Court granted certiorari to resolve a dispute as to whether one of the defendants—an attorney contracted by municipal government—was eligible for the qualified immunity afforded to his city-employed colleagues. *Id.* at 1660–61. To determine the scope of the doctrine, the Court examined “the ‘general principles of tort immunities and defenses’ applicable at common law.” *Id.* at 1662 (quoting *Imbler v. Pachtman*, 424 U.S. 409, 418 (1976)). When the examination revealed that part-time and lay officials had been granted immunity throughout the nineteenth century, *id.* at 1665, the Court concluded that the contractor was properly entitled to the same qualified immunity enjoyed by his publicly employed counterparts.

Filarsky has little to offer Campbell-Ewald. The decision is applicable only in the context of § 1983 qualified immunity from personal tort liability. *See, e.g., ibid.* (“[I]mmunity under § 1983 should not vary depending on whether an individual working for the government does so as a full-time employee, or on some other basis.”). Moreover, the Court afforded immunity only after tracing two hundred years of precedent. Here, not only do we lack decades or centuries of

common law recognition of the proffered defense, we are aware of *no* authority exempting a marketing consultant from analogous federal tort liability.

Nor are we persuaded that we should establish the novel immunity asserted by defendants. As the Supreme Court has recognized, immunity “comes at a great cost.” *Westfall v. Erwin*, 484 U.S. 292, 295 (1988), *superseded by statute on other grounds*, Pub. L. No. 100-694, 102 Stat. 4563 (1988), codified at 28 U.S.C. § 2679(d), *as recognized in Adams v. United States*, 420 F.3d 1049, 1052 (9th Cir. 2005). Where immunity lies, “[a]n injured party with an otherwise meritorious tort claim is denied compensation,” which “contravenes the basic tenet that individuals be held accountable for their wrongful conduct.” *Westfall*, 484 U.S. at 295. Accordingly, immunity must be extended with the utmost care. The record contains sufficient evidence that the text messages were contrary to the Navy’s policy permitting texts only to persons who had opted in to receive them. Consequently, we decline the invitation to craft a new immunity doctrine or extend an existing one.

VI.

As explained herein, Campbell-Ewald’s four arguments in support of summary judgment each fail. And because the motion was based on pure questions of law, we were not briefed on the factual predicates of liability. Campbell-Ewald has therefore not carried its burden to demonstrate an absence of material fact or to show that it is otherwise “entitled to judgment as a matter of law.” FED. R. CIV. P. 56(a).

Accordingly, we VACATE the district court's order and remand the case for further proceedings consistent with this opinion.

VACATED and REMANDED.

The costs shall be taxed against the Defendant-Appellee.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

)	Case No.: 13-CV-05226-LHK
)	
)	
IN RE ADOBE SYSTEMS, INC. PRIVACY)	ORDER GRANTING IN PART AND
LITIGATION)	DENYING IN PART DEFENDANT
)	ADOBE SYSTEMS INC.'S MOTION TO
)	DISMISS

In this consolidated litigation, Plaintiffs Christian Duke ("Duke"), Joseph Kar ("Kar"), Christina Halpain ("Halpain"), Jacob McHenry ("McHenry"), Anne McGlynn ("McGlynn"), and Marcel Page ("Page"), individually and on behalf of those similarly situated (collectively, "Plaintiffs") bring claims against Defendant Adobe Systems, Inc. ("Adobe") arising out of an intrusion into Adobe's computer network in 2013 and the resulting data breach. Consol. Compl. ("Compl.") ECF No. 39. Pending before the Court is Adobe's Motion to Dismiss, in which Adobe seeks dismissal of all of Plaintiffs' claims. ("Mot.") ECF No. 45. Plaintiffs have filed an Opposition, ("Opp'n") ECF No. 47, and Adobe has filed a Reply, ("Reply") ECF No. 50. Having considered the submissions of the parties and the relevant law, the Court hereby GRANTS IN PART and DENIES IN PART Adobe's Motion to Dismiss.

I. BACKGROUND

A. Factual Allegations

Except where indicated, the facts in this section are taken from Plaintiffs' Complaint and accepted as true for the purposes of this Motion.

1. Adobe's Products and Services

Adobe is a multinational software company that sells and licenses printing, publishing, multimedia, and graphics software. Compl. ¶ 17. Adobe sells a wide range of products, including Photoshop (a widely-used digital imaging program) and ColdFusion (used by web developers to build websites and Internet applications). *Id.* ¶ 19. Adobe's products and services are available in two forms. Some Adobe software, such as ColdFusion, is sold through licenses, where customers pay a single licensing fee to use the software. *Id.* Other Adobe products are available through Adobe's subscription-based "Creative Cloud," where customers pay a monthly fee to use Adobe's products and services. *Id.*

Adobe collects a variety of customer information. Customers of licensed-based products must register their products, which requires customers to provide Adobe with their e-mail addresses and create a username and password for Adobe's website. *Id.* Some of these customers purchased their licenses online from Adobe directly, and thus also provided Adobe with their credit card numbers and expiration dates, as well as other billing information. *E.g., id.* ¶¶ 19, 78, 96. Creative Cloud customers are required to keep an active credit card on file with Adobe, which is charged automatically according to the customer's subscription plan. *Id.* ¶ 19. In addition, some Creative Cloud customers store their files and work products in Adobe's "cloud." *E.g., id.* ¶ 84. As a result of the popularity of Adobe's products, Adobe has collected personal information in the form of names, e-mail and mailing addresses, telephone numbers, passwords, credit card numbers and expiration dates from millions of customers. *Id.* ¶¶ 22, 50-55.

All customers of Adobe products, including Creative Cloud subscribers, are required to accept Adobe's End-User License Agreements ("EULA") or General Terms of Use. *Id.* ¶ 29. Both incorporate Adobe's Privacy Policy, which provides in relevant part: "[Adobe] provide[s]

reasonable administrative, technical, and physical security controls to protect your information. However, despite our efforts, no security controls are 100% effective and Adobe cannot ensure or warrant the security of your personal information.” (“Agreement”) ECF No. 46-2 at 4. Adobe’s Safe Harbor Privacy Policy, which supplements Adobe’s Privacy Policy, similarly provides that “Adobe . . . uses reasonable physical, electronic, and administrative safeguards to protect your personal information from loss; misuse; or unauthorized access, disclosure, alteration, or destruction.” Compl. ¶ 32. Adobe makes similar representations regarding its security practices on its websites. *Id.* ¶¶ 33-39.

2. The 2013 Data Breach

In July 2013, hackers gained unauthorized access to Adobe’s servers. *Id.* ¶ 48. The hackers spent several weeks inside Adobe’s network without being detected. *Id.* By August 2013, the hackers reached the databases containing customers’ personal information, as well as the source code repositories for Adobe products. *Id.* The hackers then spent up to several weeks removing customer data and Adobe source code from Adobe’s network, all while remaining undetected. *Id.* The data breach did not come to light until September, when independent security researchers discovered stolen Adobe source code on the Internet. *Id.* ¶ 49. Adobe announced the data breach on October 3, 2013. *Id.* ¶ 50. Adobe announced that the hackers accessed the personal information of at least 38 million customers, including names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses. *Id.* ¶¶ 50-52. Adobe confirmed that the hackers copied the source code for a number of its products, including ColdFusion. *Id.* ¶ 53. Adobe subsequently disclosed that the hackers were able to use Adobe’s systems to decrypt customers’ credit card numbers, which had been stored in an encrypted form. *Id.* ¶ 57. The Court will refer to this sequence of events as the “2013 data breach.”

Following the 2013 data breach, researchers concluded that Adobe’s security practices were deeply flawed and did not conform to industry standards. *Id.* ¶ 59. For example, though customers’ passwords had been stored in encrypted form, independent security researchers analyzing the stolen passwords discovered that Adobe’s encryption scheme was poorly implemented, such that

the researchers were able to decrypt a substantial portion of the stolen passwords in short order. *Id.* ¶ 63. Adobe similarly failed to employ intrusion detection systems, properly segment its network, or implement user or network level system controls. *Id.* ¶ 62. As a result of the 2013 data breach, Adobe offered its customers one year of free credit monitoring services and advised customers to monitor their accounts and credit reports for fraud and theft. *Id.* ¶¶ 54, 56.

3. The Plaintiffs

Plaintiffs are customers of Adobe licensed products or Creative Cloud subscribers who provided Adobe with their personal information. Plaintiffs Kar and Page purchased licensed products directly from Adobe and provided Adobe with their names, email addresses, credit card numbers, other billing information, and other personal information. *Id.* ¶¶ 77-78, 95-96. Plaintiff McHenry purchased an Adobe licensed product, and provided Adobe with a username and password. *Id.* ¶¶ 98-99. Plaintiffs Duke, Halpain, and McGlynn subscribed to Adobe's products, and provided Adobe with their names, email addresses, credit card numbers, other billing information, and other personal information. *Id.* ¶¶ 74-75, 83-84, 90. Plaintiffs Duke, Kar, Halpain, and McGlynn are California citizens and residents. *Id.* ¶¶ 10-12, 14. Adobe informed all Plaintiffs that their personal information had been compromised as a result of the 2013 data breach. *Id.* ¶¶ 76, 80, 85, 92, 97, 100. Following the 2013 data breach, Plaintiffs Kar and Halpain purchased additional credit monitoring services. *Id.* ¶¶ 81, 86.

B. Procedural History

The seven cases underlying this consolidated action were filed in this Court between November 2013 and January 2014. *See* ECF No. 1; Case No. 13-CV-5611, ECF No. 1; Case No. 13-CV-5596, ECF No. 1; Case No. 13-CV-5930, ECF No. 1; Case No. 14-CV-14, ECF No. 1; Case No. 14-CV-30, ECF No. 1; Case No. 14-CV-157, ECF No. 1. The Court related the individual cases in December 2013 and January 2014, ECF Nos. 19, 22, 26,¹ and consolidated them on March 13, 2014, ECF No. 34. Plaintiffs filed their Consolidated Complaint on April 4, 2014. ECF No. 39. Adobe filed its Motion to Dismiss on May 21, 2014, ECF No. 45, with an

¹ Unless otherwise noted, all remaining ECF citations refer to Case Number 13-CV-5226.

1 accompanying Request for Judicial Notice, (“Def. May 21 RJN”) ECF No. 46. Plaintiffs filed their
 2 Opposition on June 11, 2014, ECF No. 47, with an accompanying Request for Judicial Notice,
 3 (“Pl. RJN”) ECF No. 48. Adobe filed its Reply on July 2, 2014, ECF No. 50, along with a second
 4 Request for Judicial Notice, (“Def. July 2 RJN”) ECF No. 51.²

5 **II. LEGAL STANDARDS**

6 **A. Rule 12(b)(1)**

7 A defendant may move to dismiss an action for lack of subject matter jurisdiction pursuant
 8 to Federal Rule of Civil Procedure 12(b)(1). A motion to dismiss for lack of subject matter
 9 jurisdiction will be granted if the complaint on its face fails to allege facts sufficient to establish
 10 subject matter jurisdiction. *See Savage v. Glendale Union High Sch.*, 343 F.3d 1036, 1039 n.2 (9th
 11 Cir. 2003). If the plaintiff lacks standing under Article III of the U.S. Constitution, then the court
 12 lacks subject matter jurisdiction, and the case must be dismissed. *See Steel Co. v. Citizens for a*
 13 *Better Env’t*, 523 U.S. 83, 101-02 (1998). In considering a Rule 12(b)(1) motion, the Court “is not

14 ² Although a district court generally may not consider any material beyond the pleadings in
 15 deciding a Rule 12(b)(6) motion, the Court may take judicial notice of documents referenced in the
 16 complaint, as well as matters in the public record, without converting a motion to dismiss into one
 17 for summary judgment. *See Lee v. City of L.A.*, 250 F.3d 668, 688-89 (9th Cir. 2001). A matter
 18 may be judicially noticed if it is either “generally known within the trial court’s territorial
 19 jurisdiction,” or “can be accurately and readily determined from sources whose accuracy cannot
 20 reasonably be questioned.” Fed. R. Evid. 201(b).

21 Here, Adobe requests that the Court take judicial notice of the transcript of the case
 22 management conference hearing held before this Court on March 13, 2014. Def. May 21 RJN Ex.
 23 A. This transcript is an appropriate subject for judicial notice, as it is a matter of public record.
 24 Adobe also requests that the Court take judicial notice of Adobe’s Privacy Policies of May 7, 2012
 25 and December 20, 2013, *id.* Exs. B, C; Adobe’s General Terms of Use, *id.* Ex. D; and the
 26 subscription terms for Adobe’s Creative Cloud, *id.* Ex. E. These documents are referenced and
 27 quoted in the Complaint, *e.g.*, Compl. ¶¶ 5, 29, 30-32, 84, 91, 99, 119-120, 129, and the Court may
 28 therefore take judicial notice of these documents under the doctrine of incorporation by reference.
See, e.g., Knievel v. ESPN, 393 F.3d 1068, 1076 (9th Cir. 2005) (district court may consider
 “documents whose contents are alleged in a complaint and whose authenticity no party questions,
 but which are not physically attached to the [plaintiff’s] pleading” (alteration in original) (internal
 quotation marks omitted)). Finally, Adobe requests that the Court take judicial notice of three
 newspaper articles discussing Adobe’s security problems. Def. July 2 RJN Exs. A, B, C. The Court
 may take judicial notice of the existence of these reports as indication of what was in the public
 realm, but not for the veracity of any arguments or facts contained within. *See Von Saher v. Norton*
Simon Museum of Art at Pasadena, 592 F.3d. 954, 960 (9th Cir. 2010). Accordingly, the Court
 GRANTS Adobe’s Requests for Judicial Notice dated May 21, 2014 and July 2, 2014.

Plaintiffs request that the Court take judicial notice of one of Adobe’s End User License
 Agreements (“EULA”). Pl. RJN Ex. A. The EULA is referenced in the Complaint, *see, e.g.*,
 Compl. ¶¶ 29-32, 41, 105, and is publicly available on Adobe’s website. Accordingly, the Court
 GRANTS Plaintiffs’ Request for Judicial Notice. *See Knievel*, 393 F.3d at 1076.

restricted to the face of the pleadings, but may review any evidence, such as affidavits and testimony, to resolve factual disputes concerning the existence of jurisdiction.” *McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988). Once a party has moved to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1), the opposing party bears the burden of establishing the court’s jurisdiction, *see Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1122 (9th Cir. 2010), by putting forth “the manner and degree of evidence required” by whatever stage of the litigation the case has reached, *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992); *see also Barnum Timber Co. v. Env’tl. Prot. Agency*, 633 F.3d 894, 899 (9th Cir. 2011) (at the motion to dismiss stage, Article III standing is adequately demonstrated through allegations of “specific facts plausibly explaining” why the standing requirements are met).

B. Rule 8(a)

Rule 8(a)(2) of the Federal Rules of Civil Procedure requires a complaint to include “a short and plain statement of the claim showing that the pleader is entitled to relief.” A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). The Supreme Court has held that Rule 8(a) requires a plaintiff to plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, a court “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

However, the Court need not accept as true allegations contradicted by judicially noticeable facts, *Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and the “[C]ourt may look beyond the plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6)

1 motion into one for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995).
 2 Nor is the Court required to “assume the truth of legal conclusions merely because they are cast in
 3 the form of factual allegations.” *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per
 4 curiam) (quoting *W. Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere “conclusory
 5 allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss.”
 6 *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004); *accord Iqbal*, 556 U.S. at 678.
 7 Furthermore, plaintiffs may plead themselves out of court if they “plead facts which establish that
 8 [they] cannot prevail on [their] . . . claim.” *Weisbuch v. Cnty. of L.A.*, 119 F.3d 778, 783 n.1 (9th
 9 Cir. 1997) (internal quotation marks and citation omitted).

10 **C. Rule 9(b)**

11 Claims sounding in fraud or mistake are subject to the heightened pleading requirements of
 12 Federal Rule of Civil Procedure 9(b), which requires that a plaintiff alleging fraud “must state with
 13 particularity the circumstances constituting fraud.” Fed. R. Civ. P. 9(b); *see Kearns v. Ford Motor*
 14 *Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009). To satisfy Rule 9(b)’s heightened standard, the
 15 allegations must be “specific enough to give defendants notice of the particular misconduct which
 16 is alleged to constitute the fraud charged so that they can defend against the charge and not just
 17 deny that they have done anything wrong.” *Semegen v. Weidner*, 780 F.2d 727, 731 (9th Cir.
 18 1985). Thus, claims sounding in fraud must allege “an account of the time, place, and specific
 19 content of the false representations as well as the identities of the parties to the misrepresentations.”
 20 *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (per curiam) (internal quotation marks
 21 omitted). “The plaintiff must set forth what is false or misleading about a statement, and why it is
 22 false.” *In re Glenfed, Inc. Sec. Litig.*, 42 F.3d 1541, 1548 (9th Cir. 1994) (en banc), *superseded by*
 23 *statute on other grounds as stated in Ronconi v. Larkin*, 253 F.3d 423, 429 n.6 (9th Cir. 2001).

24 **D. Leave to Amend**

25 If the Court determines that the complaint should be dismissed, it must then decide whether
 26 to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend
 27 “should be freely granted when justice so requires,” bearing in mind that “the underlying purpose
 28

of Rule 15 . . . [is] to facilitate decision on the merits, rather than on the pleadings or technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (internal quotation marks omitted). Nonetheless, a court “may exercise its discretion to deny leave to amend due to ‘undue delay, bad faith or dilatory motive on part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party . . . , [and] futility of amendment.’” *Carvalho v. Equifax Info. Servs., LLC*, 629 F.3d 876, 892-93 (9th Cir. 2010) (alterations in original) (quoting *Foman v. Davis*, 371 U.S. 178, 182 (1962)).

III. DISCUSSION

Plaintiffs assert four causes of action in their Complaint. Adobe seeks dismissal of all four claims. The Court will address each claim and Adobe’s corresponding objections in turn.

A. Customer Records Act Claim

Plaintiffs’ first cause of action is for injunctive relief on behalf of the California Plaintiffs for violations of Sections 1798.81.5 and 1798.82 of the California Civil Code (“CRA”).³ The CRA provides in relevant part that:

A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

Cal. Civ. Code § 1798.81.5(b). Section 1798.82, for its part, requires businesses to “disclose any breach of the security of the system following discovery or notification of the breach . . . in the most expedient time possible and without unreasonable delay.” Cal. Civ. Code § 1798.82(a).

Plaintiffs allege that Adobe did not and does not maintain “reasonable security practices” to protect customer data, in violation of Section 1798.81.5 of the CRA, and did not promptly notify

³ Adobe refers to Sections 1798.81.5 and 1798.82 as the “California Data Breach Notification Act,” see Mot. at 6, whereas Plaintiffs refer to those sections as the “California Customer Records Act,” see Opp’n at 6. The Court agrees with Plaintiffs that Section 1798.81.5 deals with more than notification in the event of a breach. See Cal. Civ. Code § 1798.81.5(d) (“[T]he purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information.”). Accordingly, the Court will refer to these sections as the Customer Records Act (“CRA”), after the name of the Title under which they appear. See Cal. Civ. Code tit. 1.81 (“Customer Records”).

customers following the 2013 data breach, in violation of Section 1798.82 of the CRA. Compl. ¶¶ 112-113.

Plaintiffs request injunctive relief pursuant to Section 1798.84(e) of the CRA, which provides that “[a]ny business that violates, proposes to violate, or has violated this title may be enjoined.” Plaintiffs also base their request for relief on the “unlawful” prong of California’s Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200 *et seq.*, which allows plaintiffs to “borrow” violations of other laws and treat them as unlawful competition that is independently actionable. *Cel-Tech Commcn’s, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999).

Adobe argues that Plaintiffs do not allege injury-in-fact resulting from Adobe’s alleged violation of the CRA and thus do not have Article III standing to bring their CRA claim. Mot. at 6-7. For the same reasons, Adobe contends that Plaintiffs do not have statutory standing under Section 1798.84(e), which also requires a showing of injury. *Id.* As a result, Adobe contends that Plaintiffs’ CRA claim must be dismissed for lack of jurisdiction. The Court addresses both contentions in turn, beginning, as it must, with Article III standing.

1. Article III Standing

To have Article III standing, a plaintiff must plead and prove that she has suffered sufficient injury to satisfy the “case or controversy” requirement of Article III of the United States Constitution. *See Clapper v. Amnesty Int’l USA*, --- U.S. ---, 133 S. Ct. 1138, 1146 (2013) (“‘One element of the case-or-controversy requirement’ is that plaintiffs ‘must establish that they have standing to sue.’” (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997))). To satisfy Article III standing, a plaintiff must therefore allege: (1) injury-in-fact that is concrete and particularized, as well as actual or imminent; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that the injury is redressable by a favorable ruling. *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010); *Friends of the Earth, Inc. v. Laidlaw Env’tl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000). “The party invoking federal jurisdiction bears the burden of

1 establishing these elements . . . with the manner and degree of evidence required at the successive
2 stages of the litigation.” *Lujan*, 504 U.S. at 561.

3 In a class action, named plaintiffs representing a class “must allege and show that they
4 personally have been injured, not that injury has been suffered by other, unidentified members of
5 the class to which they belong and which they purport to represent.” *Warth v. Seldin*, 422 U.S. 490,
6 502 (1975). “[I]f none of the named plaintiffs purporting to represent a class establishes the
7 requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or
8 any other member of the class.” *O’Shea v. Littleton*, 414 U.S. 488, 494 (1974).

9 In the instant case, Plaintiffs allege that they have all suffered at least one of three types of
10 cognizable injuries-in-fact: (1) increased risk of future harm; (2) cost to mitigate the risk of future
11 harm; and/or (3) loss of the value of their Adobe products. Opp’n at 7-11. The Court begins by
12 assessing the adequacy Plaintiffs’ alleged injuries. The Court will then address Adobe’s argument
13 that even if Plaintiffs have Article III standing to bring a claim based on Adobe’s alleged violation
14 of Section 1798.81.5 (the “reasonable” security measures provision), Plaintiffs do not have
15 standing to bring a claim based on Adobe’s alleged violation of Section 1798.82 (the notification
16 provision), because Plaintiffs do not allege that they suffered any particular injury stemming from
17 Adobe’s failure to reasonably *notify* Plaintiffs of the 2013 data breach. Mot. at 7.

18 **a. Increased Risk of Harm**

19 Plaintiffs claim that they are all at increased risk of future harm as a result of the 2013 data
20 breach. Opp’n at 7. Adobe counters that such “increased risk” is not a cognizable injury for Article
21 III standing purposes. Mot. at 10. The Ninth Circuit addressed Article III standing in the context of
22 stolen personal information in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010). In
23 *Krottner*, a thief stole a laptop from Starbucks containing the unencrypted names, addresses, and
24 social security numbers of roughly 97,000 Starbucks employees. *Id.* at 1140. Some of the affected
25 employees subsequently sued Starbucks for negligence and breach of implied contract. *Id.*
26 Starbucks argued that the employees did not have standing because there was no indication that
27 any of the employees’ personal information had been misused or that the employees had suffered
28

any economic loss as a result of the theft. *Id.* at 1141-42. The Ninth Circuit disagreed, holding instead that “the possibility of future injury may be sufficient to confer standing” where the plaintiff is “*immediately* in danger of sustaining some *direct* injury as the result of the challenged conduct.” *Id.* at 1142 (alteration omitted) (internal quotation marks omitted). As to the specific facts before it, the Ninth Circuit held that the Starbucks employees alleged “a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data.” *Id.* at 1143. Based on this “credible threat of real and immediate harm,” the Ninth Circuit found that the employees “sufficiently alleged an injury-in-fact for purposes of Article III standing.” *Id.*

Adobe does not dispute that *Krottner* is directly on point. *See* Mot. at 11; Reply at 3. However, Adobe contends that subsequent Supreme Court authority forecloses the approach the Ninth Circuit took to standing in *Krottner*. Reply at 3. Specifically, Adobe claims that the Supreme Court’s decision in *Clapper v. Amnesty International USA* expressly rejected “[a]llegations of possible future injury” as a basis for Article III standing, requiring instead that a “threatened injury [] be *certainly impending* to constitute injury in fact.” Mot. at 10 (citing *Clapper*, 133 S. Ct. at 1147). Adobe argues that following *Clapper* district courts in data breach cases regularly conclude that increased risk of future harm is insufficient to confer Article III standing under the “certainly impending” standard. *Id.* (citing *In re Sci. Applications Int’l Corp. Backup Tape Data Theft Litig.* (“SAIC”), --- F. Supp. 2d ---, 2014 WL 1858458 (D.D.C. May 9, 2014); *Strautins v. Trustwave Holdings, Inc.*, --- F. Supp. 2d ---, 2014 WL 960816 (N.D. Ill. Mar. 12, 2014); *Galaria v. Nationwide Mut. Ins. Co.*, --- F. Supp. 2d ---, 2014 WL 689703 (S.D. Ohio Feb. 10, 2014); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451 (D.N.J. 2013); *In re Barnes & Noble Pin Pad Litig.*, No. 12-8617, 2013 WL 4759588 (N.D. Ill. Sep. 3, 2013); *Yunker v. Pandora Media, Inc.*, No. 11-3113, 2013 WL 1282980 (N.D. Cal. Mar. 26, 2013)). Adobe claims that the only case to hold otherwise, *In re Sony Gaming Networks & Customer Data Security Breach Litigation*, --- F. Supp. 2d ---, 2014 WL 223677 (S.D. Cal. Jan 21, 2014), has been “relegated to a ‘*but see*’ reference.” Mot. at 11 (citing SAIC, 2014 WL 1858458, at *8). Adobe encourages this Court to conclude that *Clapper*

1 implicitly overruled *Krottner* and to join the district courts that have rejected the “increased risk of
2 harm” theory of standing in *Clapper*’s wake. *Id.* at 10-11. For the following reasons, the Court
3 declines to do so.

4 *Clapper* addressed a challenge to Section 702 of the Foreign Intelligence Surveillance Act
5 of 1978 (“FISA”), 50 U.S.C. § 1881a. 133 S. Ct. at 1142. Respondents were U.S.-based attorneys,
6 human rights, labor, legal, and media organizations who alleged that their work required them to
7 communicate with individuals outside the United States who were likely to be targets of
8 surveillance under Section 702. *Id.* at 1145. The respondents asserted injury based on “an
9 objectively reasonable likelihood that their communications [would] be acquired [under FISA] at
10 some point in the future.” *Id.* at 1146. As an initial matter, the Supreme Court held that the
11 “objectively reasonable likelihood” standard was inconsistent with precedent requiring that
12 “threatened injury must be *certainly impending* to constitute injury in fact.” *Id.* at 1147 (emphasis
13 added) (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The Supreme Court emphasized
14 that “allegations of *possible* future injury are not sufficient.” *Id.* (internal quotation marks omitted).
15 Turning to the respondents’ theory of injury, the Supreme Court found that it was both too
16 speculative to constitute “certainly impending” injury and too attenuated to be “fairly traceable” to
17 Section 702. *Id.* at 1147-48.

18 As the Supreme Court noted, the respondents did not allege that any of their
19 communications had actually been intercepted, or even that the Government sought to target them
20 directly. *Id.* at 1148. Rather, the respondents’ argument rested on the “highly speculative fear” that:

21 (1) the Government will decide to target the communications of non-U.S. persons
22 with whom they communicate; (2) in doing so, the Government will choose to
23 invoke its authority under [Section 702] rather than utilizing another method of
24 surveillance; (3) the Article III judges who serve on the Foreign Intelligence
25 Surveillance Court will conclude that the Government’s proposed surveillance
26 procedures satisfy [Section 702]’s many safeguards and are consistent with the
27 Fourth Amendment; (4) the Government will succeed in intercepting the
28 communications of respondents’ contacts; and (5) respondents will be parties to the
particular communications that the Government intercepts

Id. The Supreme Court held that this “highly attenuated” chain of possibilities did not result in a
“certainly impending” injury. *Id.* The Court observed that the first three steps of the chain

1 depended on the independent choices of the Government and the Foreign Intelligence Surveillance
 2 Court, yet the respondents could only speculate as to what decision those third parties would take
 3 at each step. *Id.* at 1149-50 (“[W]e have been reluctant to endorse standing theories that require
 4 guesswork as to how independent decisionmakers will exercise their judgment. . . .”). Moreover,
 5 respondents could not show with any certainty that *their* communications with the foreign persons
 6 allegedly under surveillance would be intercepted. *Id.* As a result, the overall chain of inferences
 7 was “too speculative” to constitute a cognizable injury. *Id.* at 1143.

8 The Supreme Court acknowledged that its precedents “do not uniformly require plaintiffs to
 9 demonstrate that it is *literally certain* that the harms they identify will come about” in order to have
 10 standing. *Id.* at 1150 n.5 (emphasis added). Rather, in some cases, the Supreme Court has found
 11 standing “based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to
 12 reasonably incur costs to mitigate or avoid that harm.” *Id.* (citing *Monsanto*, 561 U.S. at 153-54;
 13 *Pennell v. City of San Jose*, 485 U.S. 1, 8 (1988); *Blum v. Yaretsky*, 457 U.S. 991, 1000-01 (1982);
 14 *Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979)). The Supreme Court declined to overrule that
 15 line of cases. However, the Court concluded in *Clapper* that “to the extent that the ‘substantial risk’
 16 standard is relevant and is distinct from the ‘clearly impending’ requirement, respondents fall short
 17 of even that standard, in light of the attenuated chain of inferences necessary to find harm here.” *Id.*

18 *Clapper* did not change the law governing Article III standing. The Supreme Court did not
 19 overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact,
 20 causation, and redressability.⁴ *Accord Sony*, 2014 WL 223677, at *8-9 (“[T]he Supreme Court’s
 21 decision in *Clapper* did not set forth a new Article III framework, nor did the Supreme Court’s
 22 decision overrule previous precedent”). *Clapper* merely held that the Second Circuit had
 23 strayed from these well-established standing principles by accepting a too-speculative theory of
 24 future injury. *See* 133 S. Ct. at 1146 (characterizing the Second Circuit’s view of standing as
 25 “novel”). In the absence of any indication in *Clapper* that the Supreme Court intended a wide-

26 ⁴ Indeed, the “certainly impending” language can be traced back to a 1923 decision, *Pennsylvania*
 27 *v. West Virginia*, 262 U.S. 553, 593 (1923), and has been cited numerous times in U.S. Supreme
 28 Court cases addressing standing in the intervening decades. *See, e.g., Lujan*, 504 U.S. at 564 n.2;
Whitmore, 495 U.S. at 158; *Babbitt*, 442 U.S. at 298.

1 reaching revision to existing standing doctrine, the Court is reluctant to conclude that *Clapper*
2 represents the sea change that Adobe suggests. Moreover, *Clapper*'s discussion of standing arose
3 in the sensitive context of a claim that other branches of government were violating the
4 Constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually
5 rigorous as a result. *Id.* at 1147 ("Our standing inquiry has been especially rigorous when reaching
6 the merits of the dispute would force us to decide whether an action taken by one of the other two
7 branches of the Federal Government was unconstitutional." (alteration omitted) (internal quotation
8 marks omitted)).

9 "[D]istrict courts should consider themselves bound by [] intervening higher authority and
10 reject the prior opinion of [the Ninth Circuit] as having been effectively overruled" only when the
11 intervening higher authority is "clearly irreconcilable with [the] prior circuit authority." *Miller v.*
12 *Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). The Court does not find that *Krottner* and
13 *Clapper* are clearly irreconcilable. *Krottner* did use somewhat different phrases to describe the
14 degree of imminence a plaintiff must allege in order to have standing based on a threat of injury,
15 i.e., "immediate[] [] danger of sustaining some direct injury," and a "credible threat of real and
16 immediate harm." 628 F.3d at 1142-43. On the other hand, *Clapper* described the harm as
17 "certainly impending." 133 S. Ct. at 1147. However, this difference in wording is not substantial.
18 At the least, the Court finds that *Krottner*'s phrasing is closer to *Clapper*'s "certainly impending"
19 language than it is to the Second Circuit's "objective reasonable likelihood" standard that the
20 Supreme Court reversed in *Clapper*. Given that *Krottner* described the imminence standard in
21 terms similar to those used in *Clapper*, and in light of the fact that nothing in *Clapper* reveals an
22 intent to alter established standing principles, the Court cannot conclude that *Krottner* has been
23 effectively overruled.

24 In any event, even if *Krottner* is no longer good law, the threatened harm alleged here is
25 sufficiently concrete and imminent to satisfy *Clapper*. Unlike in *Clapper*, where respondents'
26 claim that they would suffer future harm rested on a chain of events that was both "highly
27 attenuated" and "highly speculative," 133 S. Ct. at 1148, the risk that Plaintiffs' personal data will
28

be misused by the hackers who breached Adobe's network is immediate and very real. Plaintiffs allege that the hackers deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates. Compl. ¶¶ 48, 50. Plaintiffs' personal information was among the information taken during the breach. *Id.* ¶¶ 76, 80, 85, 92, 97, 100. Thus, in contrast to *Clapper*, where there was no evidence that any of respondents' communications either had been or would be monitored under Section 702, *see* 133 S. Ct. at 1148, here there is no need to speculate as to whether Plaintiffs' information has been stolen and what information was taken.

Neither is there any need to speculate as to whether the hackers intend to misuse the personal information stolen in the 2013 data breach or whether they will be able to do so. Not only did the hackers deliberately target Adobe's servers, but Plaintiffs allege that the hackers used Adobe's own systems to decrypt customer credit card numbers. Compl. ¶ 57. Some of the stolen data has already surfaced on the Internet, and other hackers have allegedly misused it to discover vulnerabilities in Adobe's products. *Id.* ¶¶ 49, 70. Given this, the danger that Plaintiffs' stolen data will be subject to misuse can plausibly be described as "certainly impending." Indeed, the threatened injury here could be more imminent only if Plaintiffs could allege that their stolen personal information had already been misused. However, to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be "literally certain" in order to constitute injury-in-fact.⁵ *Clapper*, 133 S. Ct. at 1150 n.5; *see also, e.g., Monsanto*, 561

⁵ The Court further notes that requiring Plaintiffs to wait for the threatened harm to materialize in order to sue would pose a standing problem of its own, because the more time that passes between a data breach and an instance of identity theft, the more latitude a defendant has to argue that the identity theft is not "fairly traceable" to the defendant's data breach. Indeed, Adobe makes this very argument in its Motion. Specifically, Adobe speculates that Plaintiff Halpain may also have been a victim of recent data breaches involving Target and Neiman Marcus, and thus that Halpain's allegation that her personal data appeared on "black market websites" is not fairly traceable to Adobe's 2013 data breach. Mot. at 9 & n.8. This argument fails, given that there is no factual basis for Adobe's speculation that Halpain was a customer of either Target or Neiman Marcus, let alone that Halpain's personal data was compromised in data breaches involving these companies.

U.S. at 153-54 (finding that a “substantial risk of gene flow” from genetically engineered alfalfa crops to non-genetically engineered alfalfa crops was sufficient to confer Article III standing).⁶

The cases Adobe cites in which district courts have relied on *Clapper* to dismiss data breach cases on standing grounds are factually distinct from the present case. In *SAIC*, the case on which Adobe most heavily relies, a thief broke into a car in San Antonio, Texas and stole the car’s GPS and stereo, as well as encrypted backup data tapes containing personal medical information for over four million U.S. military members and their families. 2014 WL 1858458, at *2. As the *SAIC* court found, the thief would need to have recognized the data tapes for what they were, obtained specialized equipment to read the tapes, broken the encryption protecting the data on the tapes, and then obtained specialized software to read the data, all before being in any position to misuse the data. *Id.* at *6. Such a chain of possibilities, the *SAIC* court held, was as attenuated as the chain the Supreme Court rejected in *Clapper*, especially given the more likely possibility that the thief had simply sold the GPS and stereo and discarded the data tapes “in a landfill somewhere in Texas.” *Id.* The facts of *SAIC* stand in sharp contrast to those alleged here, where hackers targeted Adobe’s servers in order to steal customer data, at least some of that data has been successfully decrypted, and some of the information stolen in the 2013 data breach has already surfaced on websites used by hackers.

Adobe’s other authorities are similarly distinct. The thief in *Polanco* also stole a laptop out of a car. 988 F. Supp. 2d at 456. Again, there was no allegation that the thief targeted the laptop for the data contained therein, and the plaintiff “essentially concede[d]” that she had not alleged “any misuse of her [personal information] or [] that she [wa]s now at an increased risk for the misuse of her information in the future based on the theft of the laptop.” *Id.* at 467. In both *Strautins* and *Barnes & Noble*, it was unclear if the plaintiffs’ information had been taken at all. 2014 WL 960816, at *6-7; 2013 WL 4759588, at *4. Finally, in *Yunker*, the plaintiff did not allege that he

⁶ It is also worth noting that *Clapper* was decided on summary judgment, *see* 133 S. Ct. at 1146, which requires that a plaintiff come forward with a greater degree of evidentiary proof to support her standing allegations than is required at the motion to dismiss stage, *see Lujan*, 504 U.S. at 561.

1 had provided any sensitive information (such as a credit card number or a social security number)
2 or that anyone had breached the defendant's servers. 2013 WL 1282980, at *5.

3 The case with facts closest to those at issue here is *Galaria*. In that case, hackers obtained a
4 variety of personal information, though not credit card information, from the servers of an
5 insurance company. *Galaria*, 2014 WL 689703, at *1. The court declined to find standing based on
6 increased risk of future harm, reasoning that whether plaintiffs would be harmed depended on the
7 decision of the unknown hackers, who may or may not attempt to misuse the stolen information.
8 *Id.* at *6. The Court finds this reasoning unpersuasive—after all, why would hackers target and
9 steal personal customer data if not to misuse it?—and declines to follow it. Regardless, *Galaria*'s
10 reasoning lacks force here, where Plaintiffs allege that some of the stolen data has already been
11 misused. *See* Compl. ¶¶ 49, 70.

12 In sum, the Court finds that Plaintiffs' allegations of a concrete and imminent threat of
13 future harm suffice to establish Article III injury-in-fact at the pleadings stage under both *Krottner*
14 and *Clapper*.

15 **b. Cost to Mitigate**

16 In addition, Plaintiffs allege that Plaintiffs Halpain and Kar have standing based on the
17 reasonable costs they incurred to mitigate the increased risk of harm resulting from the 2013 data
18 breach. Opp'n at 10; *see* Compl. ¶¶ 80-81, 86-87 (alleging that Halpain and Kar paid for data
19 monitoring services). The Supreme Court held in *Clapper* that plaintiffs "cannot manufacture
20 standing merely by inflicting harm on themselves based on their fears of hypothetical future harm
21 that is not certainly impending." 133 S. Ct. at 1151. In so holding, the Supreme Court rejected the
22 *Clapper* respondents' argument that they had standing because they had taken on costly and
23 burdensome measures to protect the confidentiality of their communications. *Id.* Even where the
24 fear of harm was not "fanciful, paranoid, or otherwise unreasonable," the Supreme Court noted,
25 plaintiffs cannot secure a lower standard for standing "simply by making an expenditure based on
26 [that] fear." *Id.*

As this last quote indicates, the Supreme Court’s primary concern was that the Article III standing standard would be “water[ed] down” if a plaintiff who otherwise lacked standing could manufacture an injury-in-fact “for the price of a plane ticket.” *Id.* (internal quotation marks omitted); *accord SAIC*, 2014 WL 1858458, at *7 (“Put another way, the [Supreme] Court has held that plaintiffs cannot create standing by ‘inflicting harm on themselves’ to ward off an otherwise speculative injury.” (quoting *Clapper*, 133 S. Ct. at 1151)). Therefore, in order for costs incurred in an effort to mitigate the risk of future harm to constitute injury-in-fact, the future harm being mitigated must itself be imminent.⁷ As the Court has found that all Plaintiffs adequately alleged that they face a certainly impending future harm from the theft of their personal data, *see supra* Part III.A.1.a, the Court finds that the costs Plaintiffs Halpain and Kar incurred to mitigate this future harm constitute an additional injury-in-fact.⁸

For the foregoing reasons, the Court finds that Plaintiffs have plausibly alleged that the substantial risk of harm Plaintiffs face following the 2013 data breach constitutes a cognizable injury-in-fact. The costs Plaintiffs Halpain and Kar incurred to mitigate this risk of harm constitute an additional cognizable injury. The Court further finds that Plaintiffs plausibly allege both that these injuries are “fairly traceable” to Adobe’s alleged failure to maintain “reasonable” security measures in violation of Section 1798.81.5 and that the relief sought would redress these injuries.

⁷ The precise degree of imminence required is somewhat uncertain. While a “certainly impending” risk of future harm would undoubtedly be sufficiently imminent to confer standing on a plaintiff who took costly measures to mitigate that risk, *Clapper* did not overrule prior cases that have found standing where a plaintiff incurs costs in order to mitigate a risk of harm that is “substantial.” 133 S. Ct. at 1150 n.5 (there can be standing “based on a ‘substantial risk’ that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm”). The *Clapper* Court declined, however, to determine whether a “substantial” risk of future harm is meaningfully different from a “certainly impending” risk of future harm. *See id.* (“But to the extent that the ‘substantial risk’ standard is relevant and is distinct from the ‘clearly impending’ requirement, respondents fall short of even that standard, in light of the attenuated chain of inferences necessary to find harm here.”). This Court need not resolve whether there is any practical difference between the two formulations either, as the Court finds that Plaintiffs’ allegations meet the “certainly impending” standard.

⁸ Plaintiffs additionally allege that they suffered economic injury in the form of lost value, both because the software Plaintiffs paid for is now “highly vulnerable to attacks,” and because Plaintiffs Halpain and McGlynn would not have subscribed to Creative Cloud had they known of Adobe’s substandard security practices. *See Opp’n* at 10. As the Court has already found that all Plaintiffs have Article III standing to pursue their CRA claims based on an increased risk of harm and, in the case of Plaintiffs Halpain and Kar, costs incurred to mitigate that risk of harm, the Court need not address this additional theory of standing.

The Court therefore concludes that Plaintiffs have adequately pleaded that they have Article III standing to bring a CRA claim for violations of Section 1798.81.5.

c. Section 1798.82

Adobe argues that even if Plaintiffs have adequately alleged injury-in-fact stemming from Adobe's alleged failure to implement reasonable security measures, Plaintiffs have not alleged any injury traceable to Adobe's alleged failure to reasonably *notify* customers of the 2013 data breach in violation of Section 1798.82, because Plaintiffs do not allege that they suffered any incremental harm as a result of the delay. Mot. at 7. The Court agrees that Plaintiffs do not allege any harm resulting from the delay in their Complaint, and Plaintiffs do not address this argument in their Opposition except to argue that they have statutory (as opposed to Article III) standing to bring a Section 1798.82 claim. *See* Opp'n at 11.

Article III's standing requirements are mandatory and separate from any statutory standing requirements. Article III standing is also claim- and relief-specific, such that a plaintiff must establish Article III standing for each of her claims and for each form of relief sought. *See DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) ("[O]ur standing cases confirm that a plaintiff must demonstrate standing for each claim he seeks to press."); *id.* ("We have insisted . . . that a plaintiff must demonstrate standing separately for each form of relief sought." (internal quotation marks omitted)). Plaintiffs' claim that Adobe failed to reasonably notify its customers of the 2013 data breach is distinct from Plaintiffs' claim that Adobe failed to maintain reasonable data security measures—in that the claims arise under different statutory provisions and challenge different Adobe conduct—and Plaintiffs seek different injunctive relief to remedy each violation. *Compare* Compl. ¶ 116 (seeking injunction ordering Adobe to implement various security measures), *with id.* ¶ 117 (seeking injunction ordering Adobe to notify customers affected by the 2013 data breach who have not yet received notice that their data was stolen). Thus, the Court concludes that Plaintiffs must separately establish Article III standing under Section 1798.82. However, by failing to allege any injury resulting from a failure to provide reasonable notification of the 2013 data breach, Plaintiffs have not plausibly alleged that they have standing to pursue a

1 Section 1798.82 claim. Accordingly, the Court GRANTS Adobe's Motion to Dismiss Plaintiffs'
 2 Section 1798.82 claim for lacking of Article III standing. Because Plaintiffs may be able to cure
 3 this deficiency in an amended complaint, this dismissal is without prejudice.

4 **2. Statutory Standing**

5 The CRA also contains a statutory standing requirement. Section 1798.84, the remedies
 6 provision of the CRA, provides that "[a]ny customer injured by a violation of this title may
 7 institute a civil action to recover damages," Cal. Civ. Code § 1798.84(b), and the California Court
 8 of Appeal has held that this injury requirement applies "regardless of the remedies [a plaintiff]
 9 seek[s]," *Boorstein v. CBS Interactive, Inc.*, 222 Cal. App. 4th 456, 466-67 (2013); accord *Murray*
 10 *v. Time Inc.*, 554 F. App'x 654, 655 (9th Cir. 2014). Therefore, where a plaintiff fails to allege a
 11 cognizable injury, the plaintiff "lacks statutory standing" to bring a claim under Section 1798.84,
 12 "regardless of whether [the] allegations are sufficient to state a violation of the [statute]." *Boorstein*,
 13 222 Cal. App. 4th at 467 (internal quotation marks omitted).

14 Although Section 1798.84 does not define what qualifies as an injury under the statute,
 15 other courts in the Ninth Circuit have found that an injury that satisfies Article III's injury-in-fact
 16 standard suffices to establish statutory injury under the CRA. *See, e.g., Miller v. Hearst Commc'ns,*
 17 *Inc.*, No. 12-733, 2012 WL 3205241, at *6 (C.D. Cal. Aug. 3, 2012); *Boorstein v. Men's Journal*
 18 *LLC*, No 12-771, 2012 WL 2152815, at *3-4 (C.D. Cal. June 14, 2012). As Adobe does not
 19 contend, and as the Court has no reason to believe, that the CRA's statutory standing requirements
 20 are more stringent than Article III's, the Court finds that Plaintiffs' allegations of injury-in-fact
 21 satisfy the CRA's statutory standing requirement for the same reasons these allegations satisfy
 22 Article III. *See supra* Part III.A.1.

23 In summary, the Court DENIES Adobe's Motion to Dismiss Plaintiffs' CRA claim for
 24 violations of Section 1798.81.5. The Court GRANTS Adobe's Motion to Dismiss Plaintiffs' CRA
 25 claim for violations of Section 1798.82 without prejudice.

B. Declaratory Relief

Plaintiffs' second cause of action is for declaratory relief on behalf of all Plaintiffs. Compl. ¶¶ 118-124. As a preliminary matter, the parties disagree over whether the federal Declaratory Judgment Act, 28 U.S.C. § 2201, applies, as Adobe contends, or if the California Declaratory Relief Act, Cal. Civ. Proc. Code § 1060, applies, as Plaintiffs contend. *Compare* Reply at 5 n.4, with Opp'n at 14.

The Court finds that the federal Declaratory Judgment Act governs in this case. Although district courts in the Ninth Circuit have at times applied the California Declaratory Relief Act when sitting in diversity, *see Valley Forge Ins. Co. v. APL Co. Pte. Ltd.*, No. 09-9323, 2010 WL 960341, at *4 n.5 (C.D. Cal. Mar. 16, 2010) (citing cases), other district courts apply the federal Act, *see, e.g., DeFeo v. Procter & Gamble Co.*, 831 F. Supp. 776, 779 (N.D. Cal. 1993) ("The propriety of granting declaratory relief in federal court is a procedural matter. . . . Therefore, the Declaratory Judgment Act is implicated even in diversity cases" (citations omitted)). For its part, the Ninth Circuit has indicated, although not explicitly held, that the federal Declaratory Judgment Act should apply. In *Golden Eagle Insurance Co. v. Travelers Cos.*, 103 F.3d 750, 753 (9th Cir. 1996), *overruled on other grounds by Gov't Emps. Ins. Co. v. Dizol*, 133 F.3d 1220 (1998) (en banc), the Ninth Circuit stated that although "[t]he complaint [plaintiff] filed in state court was for declaratory relief under California's declaratory relief statute," "[w]hen [defendant] removed the case to federal court, based on diversity of citizenship, the claim remained one for declaratory relief, but the question whether to exercise federal jurisdiction to resolve the controversy became a procedural question of federal law." Finally, the U.S. Supreme Court has emphasized the procedural nature of the Declaratory Judgment Act, which further supports the conclusion that the federal Act applies. *See Skelly Oil Co. v. Phillips Petroleum Co.*, 339 U.S. 667, 671 (1950) ("[T]he operation of the Declaratory Judgment Act is procedural only." (quoting *Aetna Life Ins. Co. v. Haworth*, 200 U.S. 227, 240 (1937))). The Court will therefore consider Plaintiffs' declaratory relief claim under the federal Declaratory Judgment Act. In any event, as Plaintiffs acknowledge, whether the state or

1 federal statute applies makes little difference as a practical matter, as the two statutes are broadly
2 equivalent.⁹ *See* Opp’n at 14.

3 The federal Declaratory Judgment Act provides that “[i]n a case of actual controversy
4 within its jurisdiction . . . any court of the United States . . . may declare the rights and other legal
5 relations of any interested party seeking such declaration, whether or not further relief is or could
6 be sought.” 28 U.S.C. § 2201(a). To fall within the Act’s ambit, the “case of actual controversy”
7 must be “‘definite and concrete, touching the legal relations of parties having adverse legal
8 interests,’ . . . ‘real and substantial’ and ‘admi[t] of specific relief through a decree of a conclusive
9 character, as distinguished from an opinion advising what the law would be upon a hypothetical
10 state of facts.’” *MedImmune, Inc. v. Genentech, Inc.*, 549 U.S. 118, 127 (2007) (alteration in
11 original) (quoting *Aetna Life*, 300 U.S. at 240-241). Plaintiffs seek a declaration that: (a) Adobe
12 fails to fulfill its existing contractual obligation to provide reasonable security measures; and (b) to
13 comply with its contractual obligations, Adobe must implement specified additional security
14 measures. Compl. ¶ 124.

15 Adobe moves to dismiss Plaintiff’s declaratory relief claim on three grounds. First, Adobe
16 asserts that Plaintiffs have not suffered an injury-in-fact and therefore lack standing. Mot. at 13.
17 Second, Adobe contends that what Plaintiffs actually seek is an impermissible advisory opinion
18 that lays the foundation for future litigation, rather than adjudication of an actual controversy
19 between the parties. *Id.* at 13-14. Third, Adobe argues that Plaintiffs’ declaratory relief claim is
20 actually a breach of contract claim in disguise, and that the claim fails because Plaintiffs have
21 failed to plead all the elements of a breach of contract claim. *Id.* at 15. The Court addresses each
22 contention in turn.

23
24
25
26
27
28
⁹ Compare 28 U.S.C. § 2201 (“In a case of actual controversy within its jurisdiction . . . any court
of the United States, upon the filing of an appropriate pleading, may declare the rights and other
legal relations of any interested party seeking such declaration, whether or not further relief is or
could be sought.”), with Cal. Civ. Proc. Code § 1060 (“Any person interested under a written
instrument . . . or under a contract . . . may, in cases of actual controversy relating to the legal rights
and duties of the respective parties, bring an original action . . . for a declaration of his or her rights
and duties [T]he court may make a binding declaration of these rights or duties, whether or
not further relief is or could be claimed at the time.”).

1. Article III Standing

Adobe first claims that, just as the California Plaintiffs fail to allege injury-in-fact for purposes of their CRA claim, the California Plaintiffs fail to allege a cognizable injury-in-fact for purposes of declaratory relief. Mot. at 13; *see also Dizol*, 133 F.3d at 1222-23 (“A lawsuit seeking federal declaratory relief must first present an actual case or controversy within the meaning of Article III, section 2 of the United States Constitution. . . . It must also fulfill statutory jurisdictional prerequisites.” (citation omitted)). In addition, Adobe claims that the non-California Plaintiffs do not allege any injury whatsoever. Mot. at 13. Adobe argues that therefore none of the Plaintiffs alleges injury-in-fact that is fairly traceable to Adobe’s failure to abide by its contractual obligations. *Id.*

The Court finds that Plaintiffs have adequately pleaded that they have Article III standing to bring a claim for declaratory relief. First, as discussed above, the Court finds that all Plaintiffs have plausibly alleged that they face a substantial, “certainly impending” risk of harm from the 2013 data breach. *See supra* Part III.A.1.a. This alleged injury is fairly traceable to Adobe’s failure to abide by its contractual obligation to provide “reasonable . . . security controls,” Agreement at 4, and will plausibly be redressed by the declaratory relief Plaintiffs seek. Accordingly, the Court declines to dismiss Plaintiffs’ declaratory relief claim for lack of Article III standing.

2. Presence of an Actionable Dispute

Adobe next seeks dismissal of Plaintiffs’ declaratory relief claim on the ground that Plaintiffs do not fulfill the Declaratory Judgment Act’s statutory jurisdictional requirements. Adobe contends that there is no actionable dispute over whether Adobe is in breach of its contractual obligation to provide “reasonable . . . security controls,” given that the Agreement expressly provides that no security measure is “100%” effective and that “Adobe cannot ensure or warrant the security of your personal information.” Mot. at 14. Adobe further contends that Plaintiffs do not allege that a declaration of rights is necessary at this time. *Id.* Adobe asserts that Plaintiffs’ claim is consequently unripe, and is instead a request for an impermissible advisory opinion. *Id.* Adobe

1 contends that what Plaintiffs actually seek is an advantage for future litigation by obtaining an
2 “advance ruling.” *Id.*

3 A claim for relief under the Declaratory Judgment Act requires a dispute that is: (1)
4 “definite and concrete, touching the legal relations of parties having adverse legal interests”; (2)
5 “real and substantial”; and (3) “admit[ting] of specific relief through a decree of a conclusive
6 character, as distinguished from an opinion advising what the law would be upon a hypothetical
7 state of facts.” *MedImmune*, 549 U.S. at 127 (internal quotation marks omitted). The Supreme
8 Court has admitted that “not . . . the brightest of lines” separates cases that satisfy the statutory
9 jurisdictional requirements and those that do not. *Id.* The central question, however, is whether
10 “the facts alleged, under all the circumstances, show that there is a substantial controversy,
11 between parties having adverse legal interests, of sufficient immediacy and reality to warrant the
12 issuance of a declaratory judgment.” *Id.* (quoting *Md. Cas. Co. v. Pac. Coal & Oil Co.*, 312 U.S.
13 270, 273 (1941)).

14 The Court finds that Plaintiffs have adequately alleged the existence of an actionable
15 dispute for purposes of the Declaratory Judgment Act. Plaintiffs have plausibly alleged the
16 existence of a “definite and concrete” dispute over the meaning and the scope of Adobe’s
17 contractual obligation to provide “reasonable” security measures. *See* Compl. ¶¶ 120-123.
18 According to the Complaint, although “Adobe maintains that its security measures were adequate
19 and remain adequate,” there were in fact a number of standard industry practices that Adobe failed
20 to follow. *Id.* ¶¶ 62, 123-124. Although Adobe contends that there can be no actionable dispute
21 concerning the adequacy of Adobe’s security controls because the Agreement expressly provides
22 that no security measure is “100%” effective, Mot. at 14, this disclaimer does not relieve Adobe of
23 the responsibility (also contained in the Agreement) to provide “reasonable” security, *see*
24 Agreement at 4; Compl. ¶ 120.

25 The remaining jurisdictional prerequisites for a declaratory relief claim are met here as
26 well. The dispute over the reasonableness of Adobe’s security controls touches on the parties’ legal
27 relations, and the parties’ legal interests are adverse. *See MedImmune*, 549 U.S. at 127. Plaintiffs
28

1 plausibly allege that they face a substantial risk of future harm if Adobe's security shortcomings
2 are not redressed, making this dispute sufficiently real and immediate,¹⁰ and the dispute underlying
3 Plaintiffs' declaratory relief claim concerns Adobe's current security practices, rather than a
4 hypothetical set of acts or omissions.¹¹ *See id.*

5 Adobe contends that Plaintiffs seek an impermissible advisory opinion, claiming that
6 Plaintiffs admit that declaratory relief is necessary "only so that users . . . who suffer identity theft
7 . . . will not have to individually re-litigate the technical issue of Adobe's security obligations."
8 Mot. at 14 (emphasis removed) (citing Compl. ¶ 5). Adobe is correct that declaratory relief claims
9 brought solely for the purpose of gaining an advantage for future litigation are impermissible. *See*
10 *Calderon v. Ashmus*, 523 U.S. 740, 747 (1998). However, Plaintiffs are not seeking an advance
11 ruling on whether Adobe's security practices in 2013 were reasonable at that time. Rather, the
12 dispute is over Adobe's *current* practices. Compl. ¶ 124 ("Plaintiffs . . . seek a declaration [] that
13 Adobe's *existing* security measures do not comply with its contractual obligations" (emphasis
14 added)). Thus, the Court finds that Plaintiffs' declaratory relief claim does not merely seek an
15 advisory opinion for use in future breach of contract actions.

16 The Court concludes that Plaintiffs have plausibly alleged that they satisfy the statutory
17 jurisdictional requirements for obtaining declaratory relief. Adobe is not entitled to dismissal of
18 Plaintiffs' claim on this basis.

19
20
21 ¹⁰ Adobe contends that Plaintiffs do not allege "any adverse consequences of sufficient immediacy
22 and reality [] in the absence of their requested judicial declarations." Mot. at 14 (emphasis
23 removed). However, Plaintiffs' complaint specifically alleges that "Adobe's customers will remain
24 at risk of attack until the company completely revamps its security practices." Compl. ¶ 66.
25 Plaintiffs then substantiate this allegation of threatened harm by listing a number of Adobe's
26 allegedly unreasonable security practices, *id.* ¶ 62, and identifying previous instances in which
27 Adobe has allegedly inadequately responded to security threats, *id.* ¶¶ 43, 55.

28 ¹¹ Adobe resists this conclusion on the grounds that the remedial security measures Plaintiffs
propose do not take into account the evolving meaning of "reasonable" and are not sufficiently
specific or definitive because they refer to "industry standards" and similar undefined terms. Reply
at 6. This is unpersuasive. For one thing, the Court is not bound to adopt the precise wording of any
potential declaration set forth in a plaintiff's complaint in deciding how to award declaratory relief,
and in any event, Adobe's objections would not prevent the Court from declaring that Adobe's
current security practices are unreasonable. Such a decree would constitute "specific relief" that
would conclusively address the real dispute surrounding the scope of Adobe's existing contractual
obligations.

3. Breach of Contract Claim in “Disguise”

Adobe’s third and final challenge to Plaintiffs’ declaratory relief claim is that Plaintiffs are “seeking a declaration that Adobe has breached its contractual obligations” without having alleged all the elements of a breach of contract claim. Mot. at 15. Relying on *Gamble v. GMAC Mortgage Corp.*, No. 08-5532, 2009 WL 400359 (N.D. Cal. Feb. 18, 2009), and *Household Financial Services, Inc. v. Northern Trade Mortgage Corp.*, No. 99-2840, 1999 WL 782072 (N.D. Ill. Sept. 27, 1999), Adobe contends that Plaintiffs’ claim therefore falls outside the scope of the Declaratory Judgment Act. *Id.*

Adobe mischaracterizes Plaintiffs’ declaratory relief claim. In both *Gamble* and *Household Financial*, the plaintiffs sought a judicial decree stating that the defendants had breached their contractual obligations. *Gamble*, 2009 WL 400359, at *2 (“[P]laintiffs want the court to issue a declaratory judgment declaring that defendants breached the forbearance agreements”); *Household Fin.*, 1999 WL 782072, at *3 (“Plaintiff does not request the court to clarify the parties’ rights under the loan purchase agreement. Rather, plaintiff requests a judicial declaration that defendant breached the agreement.”). That is not what Plaintiffs seek here. As discussed above, Plaintiffs seek a declaration clarifying Adobe’s *ongoing* contractual obligation to provide reasonable security. Opp’n at 15; Compl. ¶ 124 (“Plaintiffs . . . seek a declaration [] that Adobe’s *existing* security measures do not comply with its contractual obligations” (emphasis added)). Plaintiffs’ claim thus requests precisely the type of relief that the Declaratory Judgment Act is supposed to provide: a declaration that will prevent future harm from ongoing and future violations before the harm occurs. *See, e.g. Minn. Min. & Mfg. Co. v. Norton Co.*, 929 F.2d 670, 673 (Fed. Cir. 1991) (“In promulgating the Declaratory Judgment Act, Congress intended to prevent avoidable damages from being incurred by a person uncertain of his rights and threatened with damage by delayed adjudication.”). As the Court finds that Plaintiffs are not seeking a declaration that Adobe was in breach of a contract at the time of the 2013 data breach, the Court concludes that Plaintiffs are not required to plead the elements of a breach of contract claim. The Court therefore declines to dismiss Plaintiffs’ declaratory relief claim on this basis.

For the foregoing reasons, the Court finds that Plaintiffs have plausibly pleaded that they fulfill both Article III's standing requirements and the statutory jurisdictional requirements of the Declaratory Judgment Act. The Court also finds that Plaintiffs have plausibly stated a claim for declaratory relief. Accordingly, the Court DENIES Adobe's Motion to Dismiss Plaintiffs' declaratory relief claim.

C. UCL Injunction Claim

Plaintiffs' third cause of action is for injunctive relief under the UCL on behalf of all Plaintiffs ("UCL injunction claim"). *See* Compl. ¶¶ 125-132. The UCL creates a cause of action for business practices that are: (1) unlawful, (2) unfair, or (3) fraudulent. Cal. Bus. & Prof. Code §§ 17200 *et seq.* The UCL's coverage is "sweeping," and its standard for wrongful business conduct is "intentionally broad." *In re First Alliance Mortg. Co.*, 471 F.3d 977, 995 (9th Cir. 2006) (internal quotation marks omitted). Each prong of the UCL provides a separate and distinct theory of liability. *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). To assert a UCL claim, a private plaintiff must have "suffered injury in fact and . . . lost money or property as a result of the unfair competition." *Rubio v. Capital One Bank*, 613 F.3d 1195, 1203 (9th Cir. 2010) (quoting Cal. Bus. & Prof. Code § 17204). Plaintiffs assert claims under both the "unfair" and "unlawful" prongs of the UCL. Compl. ¶ 126.

Adobe seeks dismissal of Plaintiffs' UCL injunction claim on three grounds. First, Adobe contends that Plaintiffs lack standing to bring this claim. Mot at 16. Second, Adobe contends that Plaintiffs impermissibly seek a contract remedy without bringing a breach of contract claim. *Id.* Finally, Adobe contends that Plaintiffs have failed to allege any conduct that is unfair or unlawful within the meaning of the UCL. *Id.* The Court addresses each of Adobe's contentions below.

1. Standing

Adobe argues that, just as with Plaintiffs' CRA and declaratory relief claims, Plaintiffs lack Article III standing to bring their UCL injunction claim because no Plaintiff has suffered an injury-in-fact. *Id.* For the same reason, Adobe contends that Plaintiffs lack statutory standing to bring a claim under the UCL. *Id.* The Court finds that Plaintiffs have Article III standing to bring their

1 UCL injunction claim for the same reasons that Plaintiffs have Article III standing to bring their
2 CRA and declaratory relief claims. *See supra* Part III.A.1; Part III.B.1.

3 Adobe further argues that Plaintiffs lack statutory standing under the UCL. Mot. at 16. In
4 order to establish standing for a UCL claim, plaintiffs must show they personally lost money or
5 property “as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204; *Kwikset Corp. v.*
6 *Superior Court*, 51 Cal. 4th 310, 330 (2011). “There are innumerable ways in which economic
7 injury from unfair competition may be shown. A plaintiff may (1) surrender in a transaction more,
8 or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future
9 property interest diminished; (3) be deprived of money or property to which he or she has a
10 cognizable claim; or (4) be required to enter into a transaction, costing money or property, that
11 would otherwise have been unnecessary.” *Id.* at 323.

12 Four of the six Plaintiffs allege they personally spent more on Adobe products than they
13 would had they known Adobe was not providing the reasonable security Adobe represented it was
14 providing. *See* Compl. ¶ 79 (“Had Mr. Kar known that Adobe’s security practices were inferior to
15 industry standard security practices, he would not have purchased [a] license online”); *id.* ¶ 84
16 (“Had Ms. Halpain known that Adobe employed substandard security practices, she would not
17 have subscribed to the Creative Cloud service.”); *id.* ¶ 91 (“Had Ms. McGlynn known that Adobe
18 employed substandard security practices, she would not have subscribed to the Creative Cloud
19 Service.”); *id.* ¶¶ 98-99 (“McHenry purchased Adobe Illustrator . . . for approximately \$579.99
20 [He] relied on Adobe’s Privacy Policy and believed that Adobe would provide reasonable
21 security”). Only Plaintiffs Duke and Page do not allege this or any other UCL injury.

22 The Court finds plausible Plaintiffs Kar, Halpain, McGlynn, and McHenry’s allegations
23 that they relied on Adobe’s representations regarding security to their detriment. The parties agree
24 that every Plaintiff was required to accept Adobe’s Privacy Policy before creating an account or
25 providing Adobe with their personal information. Compl. ¶¶ 31-32; Mot. at 3. In that policy,
26 Adobe represented that it would provide reasonable measures to protect customers’ personal
27 identifying and financial information. *See* Mot. at 12. It is also plausible that a company’s
28

reasonable security practices reduce the risk of theft of customer’s personal data and thus that a company’s security practices have economic value. *See Kwikset*, 51 Cal. 4th at 330 (Plaintiffs can establish UCL standing by alleging they paid more than they actually valued the product); *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1072 (N.D. Cal. 2012) (finding UCL standing was adequately pleaded where plaintiffs claimed they paid more for iPhones than they would if they had known of defendant’s alleged misrepresentations or omissions).

Accordingly, the Court finds that Plaintiffs Kar, Halpain, McGlynn, and McHenry have plausibly pleaded that they have standing to bring their UCL injunction claim. Plaintiffs Duke and Page, however, have not, though the Court cannot conclude they would be unable to cure this deficiency in an amended complaint. Accordingly, the Court GRANTS Adobe’s Motion to Dismiss Plaintiffs’ UCL injunction claim as to Plaintiffs Duke and Page without prejudice. As to the remaining Plaintiffs, Adobe is not entitled to dismissal of Plaintiffs’ UCL injunction claim on the basis of standing.

2. Contract Remedy

Adobe additionally argues that Plaintiffs’ UCL injunction claim, like Plaintiffs’ declaratory relief claim, is actually a contract claim in disguise. Mot. at 17. Specifically, Adobe claims that the UCL injunction claim is, in reality, a claim for specific performance of the Agreement. *Id.* (“Plaintiffs’ claim . . . is that Adobe should be ordered to ‘honor the terms of its contracts’ Thus, what Plaintiffs seek is the contract remedy of *specific performance*.” (quoting Compl. ¶ 129)). As specific performance is a contract remedy, Adobe contends that Plaintiffs need to plead a breach of contract claim in order to seek specific performance. *Id.* (citing *Forever 21, Inc. v. Nat’l Stores Inc.*, No. 12-10807, 2014 WL 722030, at *5 (C.D. Cal. Feb. 24, 2014); *Guidiville Rancheria of Cal. v. United States*, --- F. Supp. 2d ---, 2013 WL 6512788, at *13 (N.D. Cal. Dec 12, 2013)). Plaintiffs have not done so, and thus Adobe contends that Plaintiffs’ UCL injunction claim fails as a matter of law. *Id.*

Plaintiffs acknowledge that they have not pleaded a breach of contract claim. Opp’n at 21. Nevertheless, Plaintiffs contend that their request for an injunction is just that—a request for an

injunction under the UCL, not one for the contract remedy of specific performance. *Id.* As Plaintiffs are not seeking a contract remedy, Plaintiffs contend they do not need to plead the elements of breach of contract. *Id.*

The Court agrees with Plaintiffs that their request is indeed a request for an injunction under the UCL, and not one for specific performance. Plaintiffs do not allege that Adobe violated the UCL solely on the grounds that Adobe failed to “honor the terms of its contracts.” *See* Compl. ¶¶ 128-131. While Plaintiffs do allege “systematic breach of [] contracts” as one of Adobe’s allegedly unlawful practices, Plaintiffs also allege that Adobe’s actions are independently unlawful because they violate the duty California imposes on businesses to reasonably safeguard customers’ data under the CRA. Compl. ¶ 130; *accord* Opp’n at 21 (“Adobe’s duties arose from promises it made in its contracts and elsewhere, *and from statute.*” (emphasis added)). The Court has already determined that Plaintiffs have standing to bring claims under this statute. *See supra* Part III.A. Thus, contrary to Adobe’s assertion, Plaintiffs have alleged a basis for a UCL violation other than breach of contract. The Court therefore concludes that Plaintiffs’ request is for an injunction to remedy Adobe’s alleged UCL violations, and not to remedy an unalleged breach of contract.

3. Unlawful or Unfair

Adobe further challenges Plaintiffs’ UCL injunction claim on the ground that Plaintiffs do not plead any “unlawful” or “unfair” conduct that violates the UCL. Mot. at 18-19. The Court first considers Plaintiffs’ “unlawful” allegations, then turns to Plaintiffs’ “unfair” allegations.

a. Unlawful

The “unlawful” prong of the UCL prohibits “anything that can properly be called a business practice and that at the same time is forbidden by law.” *Cel-Tech*, 20 Cal. 4th at 180 (internal quotation marks omitted). By proscribing “any unlawful” business practice, the UCL permits injured consumers to “borrow” violations of other laws and treat them as unlawful competition that is independently actionable. *Id.* As predicates for their claim under the UCL’s “unlawful” prong, Plaintiffs allege that Adobe: (1) violated the CRA, (2) systematically breached contracts, and (3) “failed to comport with a reasonable standard of care and California public policy” as embodied in

a number of California statutes. Compl. ¶ 130 (citing the CRA, the Online Privacy Protection Act (“OPPA”), Cal. Bus. & Prof. Code § 22576, and the Information Practices Act (“IPA”), Cal. Civ. Code §§ 1798 *et seq.*).

Adobe argues that none of these allegations are adequate to sustain a UCL claim. As to Plaintiffs’ CRA allegation, Adobe contends that because Plaintiffs lack standing to bring a CRA claim, Plaintiffs similarly lack standing to pursue a UCL claim premised on a violation of the CRA. Mot. at 18. However, the Court has found that Plaintiffs *do* have standing to bring their CRA claim, and thus standing presents no barrier to Plaintiffs’ efforts to base their UCL unlawful claim on Adobe’s alleged violation of the CRA. Accordingly, the Court finds that Plaintiffs have adequately alleged unlawful conduct that may serve as a basis for a claim under the UCL’s unlawful prong, and Adobe is therefore not entitled to dismissal of the UCL unlawful claim on this basis. Because Adobe’s alleged CRA violation is sufficient to sustain Plaintiffs’ UCL unlawful claim, the Court need not address Adobe’s arguments concerning Plaintiffs’ additional allegations of unlawful conduct.

b. Unfair

The “unfair” prong of the UCL creates a cause of action for a business practice that is unfair even if not proscribed by some other law. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143 (2003). “The UCL does not define the term ‘unfair.’ . . . [And] the proper definition of ‘unfair’ conduct against consumers ‘is currently in flux’ among California courts.” *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012) (citing *Lozano*, 504 F.3d at 735). Nevertheless, there are at least two possible tests: (1) the “tethering test,” which requires “that the public policy which is a predicate to a consumer unfair competition action under the ‘unfair’ prong of the UCL must be tethered to specific constitutional, statutory, or regulatory provisions,” and (2) the “balancing test,” which examines whether the challenged business practice is “immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers and requires the court to weigh the utility of the defendant’s conduct against the gravity of the harm to

the alleged victim.”¹² *Drum v. San Fernando Valley Bar Ass’n*, 182 Cal. App. 4th 247, 257 (2010). As predicates for their claim under the UCL’s “unfair” prong, Plaintiffs allege that Adobe’s conduct fails the “balancing test” because the conduct was “immoral, unethical, . . . or substantially injurious” and caused harm that outweighed the conduct’s utility. Compl. ¶ 131. Plaintiffs further allege that Adobe’s conduct fails the “tethering test” because the conduct violated public policy as embodied in the CRA, the OPPA, and the IPA. *Id.*

Adobe contends that Plaintiffs’ claim under the “balancing test” is “conclusory and formulaic.” Mot. at 19. Specifically, Adobe claims that Plaintiffs do not allege any injuries stemming from Adobe’s allegedly unfair conduct and thus that there is no “harm” to balance against any “utility.” Reply at 9-10. As to the “tethering test,” Adobe contends that Plaintiffs’ allegations fail because Plaintiffs do not allege any violations of the OPPA or the IPA, Mot. at 19, or any effects that are “comparable to . . . a violation of” those statutes, Reply at 9 (quoting *Cel-Tech*, 20 Cal. 4th at 187).

Adobe’s argument that Plaintiffs’ “balancing test” allegations are insufficient is unpersuasive. Adobe appears to object that Plaintiffs do not allege any injuries resulting from Adobe’s allegedly unfair conduct in the precise paragraph of the Complaint asserting a claim under the “balancing test.” Mot. at 19. However, while Plaintiffs are required to plead enough facts in support of their claims, the pleading standard is not so rigid as to insist that each count repeat every factual allegation. Rather, the complaint must be specific and clear enough *as a whole* such that the Court can evaluate the plausibility of each claim and the defendant is placed on notice as to the basis for the plaintiff’s claims. *See, e.g., McVicar v. Goodman Global, Inc.*, --- F. Supp. 2d ---, 2014 WL 794585, at *7 (C.D. Cal. Feb. 25, 2014) (“[T]he thrust of [defendant’s] argument is

¹² In *Williamson v. Reinalt-Thomas Corp.*, No. 11-3548, 2012 WL 1438812, at *11 (N.D. Cal. Apr. 25, 2012), this Court recognized that the “balancing test” is sometimes construed as two separate tests. In *Williamson*, this Court noted that some California appellate courts have interpreted the balancing test to require only that a court “weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App. 4th 861, 886 (1999). On the other hand, other appellate state courts have applied a slightly different version of the balancing test, which mandates that plaintiffs show that a practice is “immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers.” *Bardin v. Daimlerchrysler Corp.*, 136 Cal. App. 4th 1255, 1260 (2006)).

1 simply to point out that under the section entitled ‘Count One: Violation of [the UCL],’ the
 2 [plaintiffs] do not specifically reference the other sections of the Complaint that identify unlawful
 3 business practices. . . . The UCL does not create such a formalistic pleading requirement.”).
 4 Elsewhere in the Complaint, Plaintiffs allege that Adobe’s conduct placed Plaintiffs at a substantial
 5 risk of future harm and caused Plaintiffs to overpay for Adobe products and services. *See, e.g.,*
 6 Compl. ¶¶ 67-73, 139. The Court has already found that these allegations of injury are sufficient
 7 for Plaintiffs to have standing to bring their UCL injunction claim. *See supra* Part III.C.1. For the
 8 same reasons, the Court finds that Plaintiffs have set forth enough factual allegations of injury to
 9 bring a claim under the “balancing test.”

10 Turning to the “tethering test,” the Court notes that contrary to Adobe’s assertion, Plaintiffs
 11 do not need to plead any direct violations of a statute to bring a claim under the UCL’s unfair
 12 prong. Instead, Plaintiffs need merely to show that the effects of Adobe’s conduct “are comparable
 13 to or the same as a violation of the law, or otherwise significantly threaten[] or harm[]
 14 competition.” *Cel-Tech*, 20 Cal. 4th at 187. Plaintiffs argue that the OPPA, the IPA, and the CRA
 15 collectively reflect California’s public policy of “protecting customer data.” Opp’n at 20. The
 16 Court agrees that California legislative intent is clear on this point, and thus finds that Plaintiffs
 17 have adequately alleged that Adobe’s conduct is “comparable” to a violation of law. *See, e.g.,* Cal.
 18 Civ. Code § 1798.1 (“The Legislature declares that . . . all individuals have a right of privacy in
 19 information pertaining to them. . . . The increasing use of computers . . . has greatly magnified the
 20 potential risk to individual privacy that can occur from the maintenance of personal information.”);
 21 Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal
 22 information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (explaining
 23 that the Legislature’s intent was to have a uniform policy state-wide regarding privacy policies on
 24 the Internet). Accordingly, the Court concludes that Plaintiffs have pleaded adequate facts to bring
 25 a claim under the “tethering test” of the UCL’s “unfair” prong.

26 In sum, the Court concludes that Plaintiffs Duke and Page have not adequately pleaded that
 27 they have standing to bring a claim under the UCL. The Court therefore GRANTS Adobe’s Motion
 28

to Dismiss this claim as to Plaintiffs Duke and Page without prejudice. However, the Court finds that Plaintiffs Halpain, McGlynn, Kar, and McHenry have adequately pleaded both standing and the necessary elements to bring their UCL injunction claim. Accordingly, the Court DENIES Adobe's Motion to Dismiss this claim as to those Plaintiffs.

D. UCL Restitution Claim

Plaintiffs' fourth and final cause of action is for restitution under the UCL on behalf of purchasers of Adobe's ColdFusion and Creative Cloud products and services ("UCL restitution claim"). *See* Compl. ¶¶ 133-140. Plaintiffs assert claims under both the "fraudulent" and "unfair" prongs of the UCL on the basis that Adobe "fail[ed] to disclose that it does not enlist industry standard security practices." Compl. ¶ 135. Adobe objects to Plaintiffs' UCL restitution claim on three grounds. First, Adobe contends that the proposed representatives of a restitution class, Plaintiffs Halpain and McGlynn, lack standing to represent ColdFusion customers as both allege only that they subscribed to Creative Cloud. Mot. at 20. Second, Adobe contends that Plaintiffs have not adequately pleaded an omission under the "fraudulent" prong of the UCL. *Id.* Third, Adobe contends that Plaintiffs have not adequately pleaded a claim under the "unfair" prong of the UCL. *Id.* at 25.

1. Standing to Bring Restitution Claims for ColdFusion Customers

Some courts reserve the question of whether plaintiffs may assert claims based on products they did not buy until ruling on a motion for class certification. *See, e.g., Forcellati v. Hyland's, Inc.*, 876 F. Supp. 2d 1155, 1161 (C.D. Cal. 2012); *Cardenas v. NBTY, Inc.*, 870 F. Supp. 2d 984, 992 (E.D. Cal. 2012). Others "hold that a plaintiff may have standing to assert claims for unnamed class members based on products he or she did not purchase so long as the products and alleged misrepresentations are substantially similar." *Miller v. Ghirardelli Chocolate Co.*, 912 F. Supp. 2d 861, 869 (N.D. Cal. 2012) (citing cases); *see also, e.g., Colucci v. ZonePerfect Nutrition Co.*, No. 12-2907, 2012 WL 6737800, at *4 (N.D. Cal. Dec. 28, 2012); *Astiana v. Dreyer's Grand Ice Cream, Inc.*, No. 11-2910, 2012 WL 2990766, at *11-13 (N.D. Cal. July 20, 2012). Still other courts have dismissed claims for lack of standing when the plaintiff did not purchase the product

on which the claim is based. *See, e.g., Granfield v. NVIDIA Corp.*, No. 11-5403, 2012 WL 2847575, at *6 (N.D. Cal. July 11, 2012) (“[W]hen a plaintiff asserts claims based both on products that she purchased and products that she did not purchase, claims relating to products not purchased must be dismissed for lack of standing.”); *Carrea v. Dreyer’s Grand Ice Cream, Inc.*, No. 10-1044, 2011 WL 159380, at *3 (N.D. Cal. Jan. 10, 2011), *aff’d on other grounds*, 475 F. App’x 113 (9th Cir. 2012).

This Court has previously applied the “substantially similar” approach and will do so again here. *E.g., Werdebaugh v. Blue Diamond Growers*, No. 12-2724, 2013 WL 5487236, at *12 (N.D. Cal. Oct. 2, 2013); *Brazil v. Dole Food Co.*, No. 12-1831, 2013 WL 5312418, at *7 (N.D. Cal. Sep 23, 2013). Under this approach, both the products themselves and the misrepresentations the plaintiff challenges must be similar, though not identical. In this case, the misrepresentations and omissions at issue are the same for both ColdFusion and Creative Cloud, as all Adobe products are governed by the same privacy policy. *See* Compl. ¶¶ 29-32. Adobe contends, however, that ColdFusion and Creative Cloud are sufficiently dissimilar *as products* that Plaintiffs lack standing to assert claims as to ColdFusion. Drawing from the Complaint, Adobe identifies the following differences between the two products: (1) ColdFusion is licensed-based whereas Creative Cloud is subscription-based; (2) customers use ColdFusion to build dynamic web sites whereas Adobe uses Creative Cloud to sell software subscriptions; and (3) ColdFusion costs up to several thousand dollars per license whereas Creative Cloud plans cost “between \$19.99 and \$79.99” a month. Mot. at 20 n.11 (citing Compl. ¶¶ 19-20). The Court notes, however, that Plaintiff Halpain alleges that she uses Creative Cloud to build websites, Compl. ¶ 89, thus suggesting that both Creative Cloud and ColdFusion can be used for website development. Therefore, assuming the Complaint’s allegations are true, as the Court must on a motion to dismiss, the Court is not persuaded by Adobe’s second-identified difference.

The Court finds that the remaining two differences between ColdFusion and Creative Cloud are not significant enough to prevent the products from being “substantially similar” for purposes of the claims alleged here. Plaintiffs’ theory of harm for their UCL restitution claim is that

ColdFusion and Creative Cloud are “heavily security-dependent” products that Plaintiffs either would not have purchased or for which Plaintiffs would not have paid as much had Plaintiffs known the truth about Adobe’s inadequate security practices. Opp’n at 17; Compl. ¶¶ 136-139. Neither the cost of a product nor whether the product is license- or subscription-based is relevant to the inquiry here, *i.e.*, whether purchasers of the products valued security, and thus whether they overpaid for their Adobe products in light of Adobe’s alleged misrepresentations and omissions regarding security. This distinguishes this case from cases applying the substantially similar approach in the food mislabeling context, where differences in the products could be expected to have an impact on whether the customer purchased the product in reliance on the defendant’s misrepresentations. *See, e.g., Larsen v. Trader Joe’s Co.*, No. 11-5188, 2012 WL 5458396, at *1, 4 (N.D. Cal. June 14, 2012) (plaintiffs lacked standing to challenge label statements on products plaintiffs did not purchase where products at issue were as disparate as cinnamon rolls, ricotta cheese, apple juice, and sandwich cookies). Accordingly, the Court concludes that Plaintiffs have pleaded sufficient facts to establish that Plaintiffs Halpain and McGlynn, the proposed representatives of a restitution class, have standing to assert claims related to both Creative Cloud and ColdFusion.

2. Fraudulent

For an omission to be actionable under the UCL, “the omission must be contrary to a representation actually made by the defendant, or an omission of a fact the defendant was obliged to disclose.” *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835 (2006); *see also Berryman v. Merit Prop. Mgmt., Inc.*, 152 Cal. App. 4th 1544, 1557 (2007) (“[A] failure to disclose a fact one has no affirmative duty to disclose is [not] ‘likely to deceive’ anyone within the meaning of the UCL.” (quoting *Daugherty*, 144 Cal. App. 4th at 838)). The California Courts of Appeal have held that there are four circumstances in which a duty to disclose may arise: “(1) when the defendant is the plaintiff’s fiduciary; (2) when the defendant has exclusive knowledge of material facts not known or reasonably accessible to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; [or] (4) when the defendant makes partial representations that are

misleading because some other material fact has not been disclosed.” *Collins v. eMachines, Inc.*, 202 Cal. App. 4th 249, 255 (2011). “[A] fact is deemed ‘material,’ and obligates an exclusively knowledgeable defendant to disclose it, if a ‘reasonable [consumer]’ would deem it important in determining how to act in the transaction at issue.” *Id.* at 256 (citing *Engalla v. Permanente Med. Grp., Inc.*, 15 Cal. 4th 951, 977 (1997)). Plaintiffs claim that Adobe had exclusive knowledge of the fact that its security practices fell short of industry standards, and that this fact was material. Opp’n at 17-18. Accordingly, Plaintiffs claim that Adobe had a duty to disclose this fact, and that Adobe’s failure to do so is an actionable omission under the UCL. *Id.*

Adobe does not dispute that facts regarding its security practices are material. Rather, Adobe contends that Adobe did not have exclusive knowledge of its security practices because Adobe’s security shortcomings were widely reported in the press before the 2013 data breach. Mot. at 21-22; Reply at 11-13. Specifically, Adobe notes that its security problems were detailed in articles published by *CNN Money*, the *New York Times*, the *Wall Street Journal*, and *Reuters*, Reply at 12, and further that Plaintiffs knew of these reports, *id.* (noting that the original individual complaints cite some of these reports); see Compl. ¶¶ 42-46 (listing security problems prior to the 2013 data breach under the heading “Adobe’s Abysmal Security Record”). Adobe notes that courts in other cases have found that defendants did not have “exclusive knowledge” of the alleged omission when the allegedly omitted fact was widely reported in similarly reputable news sources. Reply at 11-12 (citing *Herron v. Best Buy Co.*, 924 F. Supp. 2d 1161, 1175-76 (E.D. Cal. 2013) (finding that defendants did not have exclusive knowledge of battery testing conditions when those conditions had been reported in *Newsweek*); *Gray v. Toyota Motor Sales, U.S.A.*, No. 08-1690, 2012 WL 313703, at *8 (C.D. Cal. Jan. 23, 2012) (finding that defendant did not have exclusive knowledge of discrepancy between EPA estimate of car’s gas mileage and real-world results when discrepancy was reported in *Consumer Reports* and *USA Today*)). Adobe contends that “as a matter of law and logic,” Adobe could not have exclusive knowledge of the fact that it “had not implemented several industry-standard security measures.” *Id.* at 11 (internal quotation marks omitted).

The Court is not convinced. It is one thing to have a poor reputation for security in general, but that does not mean that Adobe's specific security shortcomings were widely known. None of the press reports Adobe identifies discusses any specific security deficiencies, and Plaintiffs expressly allege that the extent of Adobe's security shortcomings were revealed only *after* the 2013 data breach. Compl. ¶ 59. Given that prior reports of Adobe's security problems were highly generic, the Court cannot say that Adobe did not have exclusive knowledge of its failure to implement industry-standard security measures.¹³ Furthermore, the exact nature of what was in the public domain regarding Adobe's security practices is a question of fact not properly resolved on a motion to dismiss.

Adobe further argues that even if Plaintiffs identify an actionable omission, Plaintiffs cannot allege that they relied on that omission, as is required for a claim under the "fraudulent" prong of the UCL. Mot. at 23 (citing *In re Facebook PPC Adver. Litig.*, No. 09-3043, 2010 WL 3341062, at *9 (N.D. Cal. Aug. 25, 2010)). Adobe reasons that both Halpain and McGlynn could have cancelled their subscriptions to Creative Cloud upon learning of Adobe's security deficiencies. Mot. at 24. Neither did so, and indeed, Halpain re-subscribed to Creative Cloud after her subscription had terminated. *Id.* Adobe argues that Plaintiffs' actions are therefore inconsistent with their allegations that they would not have subscribed to Creative Cloud had they known of Adobe's security deficiencies. *Id.* (citing *Noll v. eBay, Inc.*, No. 11-4585, 2013 WL 2384250, at *4 (N.D. Cal. May 30, 2013)).

The Court disagrees. Plaintiffs allege that they would not have subscribed to Creative Cloud in the first instance had they known of Adobe's allegedly unsound security practices. Compl. ¶¶ 84, 91. Having invested time, money, and energy in Creative Cloud, however, Plaintiffs allege that the costs to switch to another product—which include early cancellation fees, *id.* ¶¶ 88, 93—are now

¹³ Adobe's reliance on *Herron* and *Gray* is misplaced. In both those cases, the press had widely reported the *exact* omission for which the plaintiffs sought to hold the defendant liable. *See Herron*, 924 F. Supp. 2d at 1175-76 (no actionable omission where both the defendant and the press had reported the testing conditions used to measure a laptop's battery life); *Gray*, 2012 WL 313703, at *8 (no actionable omission where press reported that the EPA's gas mileage estimates for the Toyota Prius were significantly higher than real-world experience). There is no such specificity here.

too high to justify abandoning their Creative Cloud subscriptions. *See* Opp’n at 19 (citing Compl. ¶ 137). This is a plausible allegation. Moreover, a plaintiff need not allege that a product became totally worthless to her once the defendant’s misrepresentation came to light in order to plead actionable reliance. Rather, it is enough to allege that the product is worth *less* to the plaintiff in light of the misrepresentation. *See Kwikset*, 51 Cal. 4th at 330 (plaintiff may establish reliance by alleging that she “paid more than . . . she actually valued the product”). Thus, Plaintiffs need not have concluded that Creative Cloud is completely worthless, and thus have canceled their subscriptions, in order to have detrimentally relied on Adobe’s alleged misrepresentations or omissions regarding security.¹⁴ Accordingly, the Court finds that Plaintiffs have not pleaded themselves out of court by alleging that they did not cancel their Creative Cloud subscriptions upon learning of Adobe’s omissions regarding security.

For these reasons, the Court concludes that Plaintiffs have adequately pleaded that Adobe had a duty to disclose that its security practices were not up to industry standards, that this omission was material, and that Plaintiffs relied on this omission to their detriment. Thus, Plaintiffs have adequately pleaded their UCL restitution claim under the UCL’s “fraudulent” prong, and Adobe is not entitled to dismissal of this claim.

3. Unfair

Plaintiffs also assert two claims under the UCL’s “unfair” prong for their UCL restitution claim. First, Plaintiffs allege that Adobe’s competition invested in industry-standard security practices, and therefore Adobe gained an unfair competitive advantage to the extent that Adobe did not. Compl. ¶ 138. Plaintiffs contend that this conduct was “unethical, unscrupulous, and

¹⁴ Adobe’s authority is not to the contrary. In *Noll*, the plaintiffs alleged that defendant eBay failed to disclose that listing fees automatically recurred every 30 days. 2013 WL 2384250, at *2. Critically, the *Noll* plaintiffs did not allege that they would incur any costs, direct or hidden, if they cancelled their listings. *Id.* Yet the *Noll* plaintiffs continued to pay the listing fees even after they discovered that the fees recurred automatically. *Id.* Their behavior after discovering the omission was therefore exactly the same as their behavior before they knew of the omission, logically foreclosing any allegations of reliance. *Id.* at *4. Here, in contrast, Plaintiffs plausibly allege that they faced costs to cancelling their subscriptions and to not re-subscribing that they did not face when deciding whether to subscribe to Creative Cloud in the first place.

substantially injurious.” *Id.* Second, Plaintiffs allege that Adobe’s conduct undermined California public policy as embodied in the OPPA, the IPA, and the CRA. *Id.*

Adobe’s objection to these claims again is that Plaintiffs did not include all of the factual allegations supporting these claims in the section of the Complaint that lays out the UCL restitution claim. *See* Mot. at 25; Reply at 15. As previously discussed, *see supra* Part III.C.3.b., the pleading standard does not require that every factual allegation needs to be repeated for every cause of action, *e.g. McVicar*, 2014 WL 794585, at *7. Elsewhere in the Complaint, Plaintiffs identify a number of specific industry-standard security measures that Adobe allegedly did not implement, Compl. ¶ 62, and allege that Adobe’s competitors did invest in these measures, *id.* ¶ 138; *see also id.* ¶ 60 (“[C]ompanies like Adobe that do business with major financial institutions or credit card issues must certify that their security measures and protocols are compliant with [an industry standard].”). Plaintiffs therefore plausibly allege that Adobe gained an unfair competitive advantage by not spending money on security the way its competitors did. Plaintiffs also plausibly allege that they were injured by Adobe’s conduct in that they overpaid for Adobe products as a result. *Id.* ¶ 139.

Adobe also repeats the argument that Plaintiffs’ “public policy” allegations are flawed because Plaintiffs do not plead violations of the OPPA, the IPA, and the CRA. Mot. at 25. As previously discussed, *see supra* Part III.C.3.b, the “unfair” prong does not require Plaintiffs to plead direct violations of these statutes. Instead, the Court has already found that Plaintiffs plausibly allege that the OPPA, the IPA, and the CRA reflect California’s policy objective of reasonably securing customer data. *See supra* Part III.C.3.b. Plaintiffs further plausibly allege that Adobe’s purported failure to provide industry-standard security undermines that policy objective. The Court therefore finds that Plaintiffs have pleaded with sufficient specificity all the necessary elements of a claim under the UCL’s “unfair” prong for their UCL restitution claim, and Adobe is not entitled to dismissal of the claim on that basis.

For the foregoing reasons, the Court DENIES Adobe’s Motion to Dismiss Plaintiffs’ UCL restitution claim.

IV. CONCLUSION

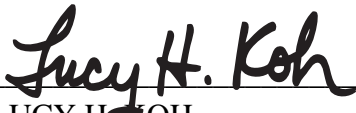
For the reasons discussed above, the Court:

1. GRANTS Adobe's Motion to Dismiss Plaintiffs' CRA claim for violations of Section 1798.82 without prejudice;
2. GRANTS Adobe's Motion to Dismiss Plaintiffs' UCL injunction claim as to Plaintiffs Duke and Page without prejudice; and
3. DENIES the remainder of Adobe's Motion to Dismiss.

Should Plaintiffs elect to file a Second Amended Complaint curing the deficiencies identified herein, Plaintiffs shall do so within thirty days of the date of this Order. Failure to meet the thirty-day deadline to file an amended complaint or failure to cure the deficiencies identified in this Order will result in a dismissal with prejudice. Plaintiffs may not add new causes of actions or parties without leave of the Court or stipulation of the parties pursuant to Federal Rule of Civil Procedure 15.

IT IS SO ORDERED.

Dated: September 4, 2014



LUCY H. KOH
United States District Judge

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Present: The Honorable	CHRISTINA A. SNYDER	
Catherine Jeang	Laura Elias	N/A
Deputy Clerk	Court Reporter / Recorder	Tape No.
Attorneys Present for Plaintiffs:		Attorneys Present for Defendants:
James Hannink		Angela Agrusa
James Clapp		
Zev Zysman		
Proceedings:	MOTION FOR CLASS CERTIFICATION (Docket #54, filed April 30, 2014)	

I. INTRODUCTION

Plaintiffs Steven Ades (“Ades”) and Hart Woolery (“Woolery”) filed the instant putative class action on March 15, 2013 in Los Angeles County Superior Court. Defendant in this action is Omni Hotels Management Corporation (“Omni”). Omni removed the case to this Court based on diversity of citizenship on April 8, 2013. Dkt. #1. Plaintiffs have since sought to substitute Jonathan Murphy (“Murphy”) for Woolery as class representative. Dkt. #55, 59.

On April 29, 2013, plaintiffs filed a First Amended Complaint (“FAC”). The FAC asserts claims for relief pursuant to the California Invasion of Privacy Act (“CIPA”), California Penal Code § 630 *et seq.* In brief, these claims assert that plaintiffs called Omni’s toll-free telephone numbers and provided Omni representatives with personal information. FAC ¶¶ 16 – 17. Plaintiffs allege that when they placed their calls to Omni’s toll-free telephone numbers, they were not apprised that the call might be recorded. *Id.* Plaintiffs further allege that Omni has a company-wide policy of recording inbound telephone conversations with consumers without seeking permission or informing consumers about the monitoring. *Id.* ¶¶ 18 – 19.

On April 30, 2014, plaintiffs filed a motion for class certification. Dkt. #54. Omni filed an opposition on July 16, 2014. Dkt. #62. Plaintiffs replied on August 25, 2014.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

#71. The parties appeared at oral argument on September 8, 2014. Following the hearing, Omni submitted a supplemental declaration, Dkt. #77, and a supplemental brief addressing a hypothetical posed during argument, Dkt. #78. After considering the parties' arguments, the Court finds and concludes as follows.

II. BACKGROUND

Plaintiffs contend that they called Omni's toll-free phone number and, without being warned that their calls were being recorded, provided Omni representatives with personal information including their names, phone numbers, e-mail addresses, and credit card numbers and expiration dates. FAC ¶¶ 16-17. Plaintiffs allege that unwarned and unconsented recording and monitoring of inbound calls pursuant to Omni company policy violated § 632.7 of CIPA, entitling them to statutory damages. *Id.* ¶¶ 31-46. Plaintiffs seek to certify a class of

All individuals who, between March 15, 2012 and March 22, 2013, inclusive (the "Class Period"), while physically present in California, participated in a telephone call with a live representative of Omni that was: (1) placed to [one of several Omni toll-free numbers], (2) made from a telephone number that includes a California area code; and (3) transmitted via cellular telephone on the network of AT&T, Verizon Wireless, or Sprint. The class excludes all employees of defendant and plaintiffs' counsel and their employees.

Dkt. #59.

A. Omni's Call Center

Omni owns a chain of approximately fifty hotels and resorts. At issue are calls placed to Omni's Customer Contact Center ("Call Center") in Omaha, Nebraska, regarding hotel reservations. L. Reynolds Decl. ¶ 2. During the Class Period, it was Omni's policy to record all calls to the toll-free phone numbers listed in the putative class definition. Liu Depo. at 100:24 - 102:11. According to Omni, these calls were used for the sole purpose of ensuring quality customer service. L. Reynolds Decl. ¶ 3. Omni did not record outgoing calls placed by its agents to customers. Korner Decl. ¶ 2.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Approximately 900,000 call recordings have been preserved from the Class Period, and Omni’s records reflect calls from approximately 40,000 telephone numbers with California area codes during that time. Id. ¶ 5; Levitan Decl. ¶ 22.

Omni did not have a policy during the Class Period of warning callers that their calls would be recorded. Resp. Ades Interrog. #9, at 9. On March 25, 2013, after learning of this lawsuit, Omni began playing an automated warning at the outset of all calls received at the Call Center: “To ensure quality service, this call may be monitored or recorded.” Id. The Call Center’s General Manager has stated that during the Class Period, Reservation Agents were permitted to tell callers they were being recorded if asked, but were not instructed to advise callers otherwise. Liu Decl. at 105:2-15; Def.’s Resp. Woolery Interrog. #15. The same manager stated that he is not aware of any documents provided to callers during the Class Period warning that calls may be monitored or recorded. Liu Decl. at 103:12 - 104:5. In response to discovery requests, Omni has not identified any callers who were advised their calls were being recorded, but maintains that callers “knew or were generally aware that their calls were being recorded.” Def.’s Resp. Woolery Interrog. #15.

B. Omni’s Monitoring and Record Keeping Systems

During the Class Period, Omni used an automated phone system called “Aspect” to direct inbound calls to reservation agents. The Aspect system also documented incoming call information including the telephone number of the caller, the Omni extension that was called, the name of the agent who handled the call, and the date, start time, and duration of the call. Liu Depo. at 154:1 - 155:19. During the Class Period, Omni also used a system called “Qfiniti,” which recorded and stored telephone calls as WAV audio files and compiled related call detail data. Resp. Woolery Req. Admis. #1-3 (Pl.’s Ex. 6) at 145-46. Finally, Omni used a system called “Opera” to record call information relating to reservations. The Opera system recorded some information automatically, including the date and time the reservation was made. Liu Depo. at 247:7-17. Reservation Agents manually entered other information pertaining to reservations into the Opera system. Using Opera records, Omni has produced data concerning approximately 36,000 reservations made during the Class Period associated with telephone numbers with California area codes. Id. at 227:19 - 228:9. These associated telephone numbers were not necessarily the same telephone numbers used to make the reservation. Id. at 228:4-9.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Additionally, Omni has provided evidence that less than 50% of calls to the Call Center result in reservations, that an unspecified “large percentage” of callers call on behalf of someone else, and that the name of the caller is “frequently” not entered in reservation records. See Etherington Decl. ¶¶ 8-9. A computer specialist consulted by Omni has stated that slightly less than half of the reservation records “have at least some information entered in one or both of the ‘caller name’ fields.” Okhandiar Decl. ¶ 7b.

Omni maintains that despite the policy of recording all incoming calls to the Call Center during the Class Period, a significant number of calls were not actually recorded.¹ Omni has provided evidence that the Qfiniti system consisted of twenty-one different services (*e.g.*, separate screen capture and voice recording programs), and that when one or more services went down, the entire Qfiniti system had to be taken offline, during which time no calls were recorded. See Korner Decl. ¶ 4c. Omni’s IT Support Manager for the Call Center stated that as a result, an unknown but “not insubstantial” number of calls were not recorded. Id. The recording system was also offline for approximately seven minutes every three months during quarterly Windows updates. Korner Decl. ¶ 4d; Korner Depo. at 36:2-14. Additionally, it took some time for new Reservation Agents to be added to the Qfiniti system, during which time any calls allocated to those new agents were not recorded. Korner Decl. ¶ 4e. An Omni agent has stated that this could “last all day or an entire weekend without being cured.” Id. Another of Omni’s employees has stated that he is aware of “several situations” in which, for unknown reasons, Omni was unable to access calls that should have been recorded. Liu Depo. 116:17 - 117:23. Another Omni employee who started as a Reservation Agent has stated that her efforts to pull recordings made during the Class Period were unsuccessful approximately 30% of the time. Etherington Decl. ¶ 6.

Omni maintains that it is impossible to determine which specific calls were not recorded due to these various technical issues. Korner Decl. ¶ 4. One Omni employee

¹Initially, Omni contended that for nearly three months of the class period, the installation of a new T-1 line caused twenty percent of the calls not to be recorded. See Mem. Opp’n Class Cert. at 19; Korner Decl. ¶¶ 2-6. However, Pat Korner has since declared that the new T-1 line was not installed until April 11, 2013, after the close of the Class Period. See Korner Suppl. Decl. ¶¶ 2-4.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

explained that although documents in Omni’s “ticketing system” could identify some periods during which a system glitch would have prevented the recording of telephone calls, not all glitches were ticketed and those that were ticketed would not directly reflect the calls not recorded. Korner Depo. at 28:2-23. Omni has produced a list of “tickets referencing the Qfiniti system during the Class Period and indicating that calls were not recorded.” See Korner Suppl. Decl. Ex. A. This list notes thirty-nine instances of problems that could have affected call recording or call detail capture, but Omni states that it cannot tell which data were not recorded as a result, and that other glitches were not ticketed at all. Id.

C. Retention and Search Functionality of Call Records

Aspect call records can be searched by the telephone number of the caller or receiving line; the date, start, or end time of the call; or the name of the agent who handled the call. Liu Depo. at 155:23 - 156:24. These call records do not, however, include the identity of the actual caller, the geographic origin of the call, the carrier that routed the call, whether the caller was using a cellular or landline phone, or whether the call was recorded. Korner Decl. ¶ 6. Moreover, as explained below, the Qfiniti audio recordings and related call data for the Class Period are not easily searchable.

Omni has provided evidence that upon learning of the filing of the lawsuit, it asked IT employee Pat Korner to preserve call recordings that had not already been automatically deleted. Korner Decl. ¶ 10. During the Class Period, the Omni system was set to automatically delete call recordings and related data within 140 to 180 days of the call date, depending on whether the call recording was listened to by a specialist. Korner Decl. ¶ 11; Korner Depo. at 100:22 - 101:10.² Automatically deleted or “aged” data cannot be recovered. Maly Decl. ¶ 9. Korner turned off this “aging function” immediately upon being told of the litigation. Korner Decl. ¶ 10. He then contacted the Qfiniti vendor with whom Omni had a service contract for help in preserving the call recordings and related data. Id. ¶ 14. Korner stated that he explained to Qfiniti that he

²Omni contends that plaintiffs’ counsel did not send Omni a litigation hold letter before filing the lawsuit, which plaintiffs have not disputed. See Korner Decl. ¶ 11; Mem. Opp’n Class Cert. at 5-6.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

“needed to preserve indefinitely the WAV file folders containing the Class Period recordings and all related call detail stored in Qfiniti.” Id. ¶ 15. Pursuant to instructions from Qfiniti, and after Qfiniti staff had classified the records as “do not delete,” Korner moved the records to a separate storage system. Id. ¶ 17. Qfiniti attempted to run a test to ensure that the records had been successfully preserved, but this test failed because of insufficient Random Access Memory. Id. Korner then marked the audio recordings “read only” as an additional protection against automatic deletion. Id. ¶ 19.

The audio recordings were successfully moved to the separate storage and remain preserved along with screen capture data reflecting “all information typed into the Omni reservation system by the Reservation Agent,” including the agent name, date and time of call, name on reservation, and billing address. Korner Decl. ¶ 18. Omni possesses audio recordings of 493,584 calls made during the Class Period. Resp. Ades Interrog. #10, at 4. However, the “do not delete” reclassification performed by Qfiniti failed for apparently unknown reasons, resulting in the loss of related call detail records and attendant search functionality when the aging function was reactivated. Korner Decl. ¶¶ 19, 24. Korner states that he did not realize the mistake had been made until approximately seven months after the preservation efforts. Korner Depo at 144:25 - 145:25. Because all Qfiniti call data is deleted within 180 days, this means that the linked call detail database for all calls made during the Class Period has been destroyed.

Korner and an expert retained by Omni maintain that relying on Qfiniti’s support service was reasonable and in line with industry standards. Korner Decl. ¶ 12; Garrie Decl. ¶¶ 12-13, 16. But plaintiffs’ expert, John Maly (“Maly”), criticizes Korner and Omni’s preservation efforts on several grounds. First, Maly submits that it was unreasonable for Omni to rely on Korner, who was not extensively trained in Qfiniti, to preserve the records. Maly Decl. ¶ 18. Maly also maintains that Omni operated Qfiniti system with insufficient disk space. Id. ¶ 20. Maly contends that Korner should have consulted the Qfiniti manual instead of relying on Qfiniti support, and should have begun the preservation process by making a complete backup of the call data. Id. ¶¶ 19, 27. Further, Maly maintains that the failed test should have prompted Korner to take the system offline and explore other preservation methods, including applying the “read-only” classification to the call detail data, and that Omni should have performed other tests to ensure the relevant data was preserved. See id. ¶¶ 14-15, 28-32. Korner responds that Qfiniti representatives were confident that their “do not delete” classification would

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

succeed in preserving the call detail data, and that applying the “read-only” classification to the call detail data as Korner did for the audio recordings would have interfered with ongoing recording operations. Korner Decl. ¶ 24. Korner also denies that Omni operated the Qfiniti server with insufficient disk space. Id. ¶ 28.

The parties and their experts disagree on the scope of search functionality lost when Qfiniti’s preservation attempts failed. Maly contends that the deletion of the call detail data severely hampered the searchability of the audio recordings, which are now unclassified. Maly Decl. ¶ 16. If the data had been preserved, plaintiffs argue, Omni could have easily accessed all of the audio recordings made from telephone calls with California area codes. Id. ¶ 6. Moreover, plaintiffs argue that if Omni had acquired and used an optional Qfiniti voice recognition feature, the parties could have searched the calls by relevant words or phrases. Id. Omni does not currently, and during the Class Period did not, have this add-on search feature. Liu Depo. at 238:8 - 239:25. Korner has stated that he has “no reason to believe” that the add-on search functionality could be applied after the fact to recordings made before installation of the upgrade. Korner Decl. ¶ 21. Omni has submitted evidence that without this add-on functionality, even had all records been completely preserved, they could not have been searched by key words spoken during a conversation, but rather only by “the caller’s telephone number, the telephone number called, the time and date the call was received, the duration of the call and the name of the Reservation Agent.” Id. ¶ 20. Moreover, Omni argues that all of the data lost is available and searchable by other means. The preserved call recordings can be searched by date and time, and Omni has produced data reflecting the telephone number, date and time, Reservation Agent, and reservation customer name (if any) for each call made during the Class Period. Id. Plaintiffs submit that although the records would have been more easily searchable had Omni done more to protect the evidence, they can still be searched sufficiently to make the class action manageable. See Okhandiar Decl. ¶ 9 (explaining initial efforts to link Aspect and Opera information). Plaintiffs point out that Omni was able to search for and locate the calls of Ades and Woolery soon after learning of the lawsuit. See Liu Depo. at 213:23 - 214:5.

D. The Putative Class Representatives

Ades placed a call to one of Omni’s toll-free reservation numbers on January 9, 2013. Ades Decl. ¶ 5. Ades placed the call using a cordless handset in conjunction with

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

a “Home Phone Connect” system from Verizon Wireless, which transmitted the call over the Verizon Wireless cellular network. Id. ¶ 7. He has declared that he did not receive any warning that the call would be recorded, did not know Omni was recording the call, and did not consent to being recorded. Id. ¶ 5. Murphy called one of Omni’s toll-free reservation numbers on June 11, 2012, using a cellular telephone serviced by the AT&T wireless network. Murphy Decl. ¶ 5. Murphy has declared that he was not told Omni was recording his calls and neither knew about nor consented to being recorded. Id.

III. LEGAL STANDARD

“Class actions have two primary purposes: (1) to accomplish judicial economy by avoiding multiple suits, and (2) to protect rights of persons who might not be able to present claims on an individual basis.” Haley v. Medtronic, Inc., 169 F.R.D. 643, 647 (C.D. Cal. 1996) (citing Crown, Cork & Seal Co. v. Parking, 462 U.S. 345 (1983)). Federal Rule of Civil Procedure 23 governs class actions and requires a “rigorous analysis.” Gen. Tel. Co. of the Sw. v. Falcon, 457 U.S. 147, 161 (1982).

To certify a class action, plaintiffs must set forth facts that provide prima facie support for the four requirements of Rule 23(a): (1) numerosity; (2) commonality; (3) typicality; and (4) adequacy of representation. Wal-Mart Stores, Inc. v. Dukes, 564 U.S. ---, ---, 131 S.Ct. 2541, 2548 (2011); Dunleavy v. Nadler (In re Mego Fir. Corp. Sec. Litig.), 213 F.3d 454, 462 (9th Cir. 2000). These requirements effectively “limit the class claims to those fairly encompassed by the named plaintiff’s claims.” Falcon, 457 U.S. at 155 (quoting Califano v. Yamasaki, 442, U.S. 682, 701 (1979)).

If the Court finds that the action meets the prerequisites of Rule 23(a), the Court must then consider whether the plaintiffs have satisfied “through evidentiary proof at least one of Rule 23(b)’s provisions.” Comcast Corp. v. Behrend, 133 S.Ct. 1426, 1432 (2013). Rule 23(b)(3) governs cases where monetary relief is the predominant form of relief sought, as is the case here. A class is maintainable under Rule 23(b)(3) where “questions of law or fact common to the members of the class predominate over any questions affecting only individual members,” and where “a class action is superior to other available methods for fair and efficient adjudication of the controversy.” Fed. R. Civ. P. 23(b)(3). “The Rule 23(b)(3) predominance inquiry tests whether the proposed classes are sufficiently cohesive to warrant adjudication by representation.” Hanlon v.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Chrysler Corp., 150 F.3d 1011, 1022 (9th Cir. 1998) (citing Amchem Products, Inc. v. Windsor, 521 U.S. 591 (1997)). The predominance inquiry measures the relative weight of the common to individualized claims. Id. “Implicit in the satisfaction of the predominance test is the notion that the adjudication of common issues will help achieve judicial economy.” Zinser v. Accufix Research Inst., Inc., 253 F.3d 1180, 1189 (9th Cir. 2001) (citing Valentino v. Carter-Wallace, Inc., 97 F.3d 1227, 1234 (9th Cir. 1996)). In determining superiority, the court must consider the four factors of Rule 23(b)(3): (1) the interests members in the class have in individually controlling the prosecution or defense of the separate actions; (2) the extent and nature of any litigations concerning the controversy already commenced by or against members of the class; (3) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (4) the difficulties likely encountered in the management of a class action. Id. at 1190–1993. “If the main issues in a case require the separate adjudication of each class member’s individual claim or defense, a Rule 23(b)(3) action would be inappropriate.” Id. (citing 7A Charles Alan Wright, Arthur R. Miller & Mary Kay Kane, Federal Practice and Procedure § 1778 at 535–39 (2d. 3d. 1986)).

More than a pleading standard, Rule 23 requires the party seeking class certification to “affirmatively demonstrate . . . compliance with the rule—that is he must be prepared to prove that there are in fact sufficiently numerous parties, common questions of law or fact, etc.” Dukes, 131 S.Ct. at 2551. This requires a district court to conduct “rigorous analysis” that frequently “will entail some overlap with the merits of the plaintiff’s underlying claim.” Id.

IV. ANALYSIS**A. Whether the Class is Ascertainable**

Omni argues that even if the requirements of Rule 23 discussed below are met, certification is not appropriate because the classes are not ascertainable. “Although there is no explicit requirement concerning the class definition in [Rule 23], courts have held that the class must be adequately defined and clearly ascertainable before a class action may proceed.” Wolph v. Acer Am. Corp., 272 F.R.D. 477, 482 (N.D. Cal. 2011). An ascertainable class exists if it can be identified “by reference to objective criteria.” Parkinson v. Hyundai Motor Am., 258 F.R.D. 580, 593 (C.D. Cal. 2008).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Plaintiffs argue that the proposed class definition sets forth objective criteria by which individuals can identify themselves as members of the class and the court can administratively determine who is a class member. They argue that the Omni Aspect list and telecommunications databases can be used to identify phone calls to Omni during the Class Period associated with California cellular telephone numbers, and that reverse lookup directories or wireless carrier records can be used to identify callers on the Verizon Wireless, AT&T Wireless, and Sprint cellular networks. Plaintiffs contend that the physical location of the caller at the time of the call can be determined objectively through records of the wireless carrier that handled each call, and that reservation records can also help identify class members. Finally, plaintiffs assert that any difficulties in identifying class members are attributable to Omni’s destruction of data that could have been used to search the audio recordings, and that it would be unfair to allow such difficulties to prejudice class certification.

Omni denies that the proposed class can be ascertained without resort to individualized, fact-intensive questions. First, Omni contends that many calls during the class period were not recorded due to technical problems and cannot be easily separated from calls that were recorded. Second, Omni argues that the mobility of cellular phones makes it impossible to determine on a classwide basis which calls from California telephone numbers were made while the putative class member was physically in California. To the extent that plaintiffs rely on wireless carrier records for such determinations, Omni argues that plaintiffs “have not met their burden to demonstrate that those private records will *actually be produced* and that they will be *complete and accurate*.” Mem. Opp’n Class Cert. at 20.³ Omni submits that the imprecision of cell site location data would create additional uncertainty for any calls placed from near any of California’s borders. Finally, Omni argues that even if records indicate the identify of the cell phone numbers at issue, that does not establish the identify of the *callers* on a classwide basis. Omni contends that family members, assistants, and other people borrow and use cell phones to make calls, and that the name of the guest on a reservation record is often distinct from the person who made the reservation over the telephone.

³In particular, Omni avers that Sprint call data was not preserved between March and July of 2012. See First Keep Decl. ¶ 3.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Plaintiffs respond that the vast majority of calls were indisputably recorded and that, to the extent Omni can produce evidence that specific calls were not, those callers can be excluded from the class. Plaintiffs reiterate that the origin of calls can be shown by cell site location data, and argue that courts routinely certify California-only classes despite the absence of commercial records independently documenting residency.

The Court does not find a lack of ascertainability to defeat class certification here. Courts in this circuit have found it “enough that the class definition describes a set of common characteristics sufficient to allow a prospective plaintiff to identify himself or herself as having a right to recover based on the description.” McCrary v. The Elations Co., LLC, No. EDCV 13-00242 JGB (OPx), 2014 WL 1779243, at *8 (C.D. Cal. Jan. 13, 2014). Plaintiffs’ class definition sets forth objective characteristics sufficient to enable prospective class members to identify themselves. The definition limits the class to those who made a call within a certain time period, while located in a specific geographic area, from a cellular phone, on one of three wireless networks, to a particular set of toll-free telephone numbers. Potential class members can show that they fit the class definition through records identified by plaintiffs showing that the putative class members’ qualifying cellular telephones were used to call one of the specified Omni lines from California during the Class Period.

To the extent that Omni has evidence that some of these calls were not recorded or were not placed from California or by the putative plaintiff, Omni can offer that evidence to disqualify class members. And district courts may narrow or decertify a class before final judgment. See F. R. Civ. P. 23(c)(1)(C). But the possibility that Omni may be able to disqualify some putative class members if more evidence comes to light does not make the class unascertainable: “in the Ninth Circuit there is no requirement that the identify of the class members . . . be known at the time of certification.” Werdebaugh v. Blue Diamond Growers, No. 12-cv-2724-LHK, 2014 WL 2191901, at *11 (N.D. Cal. May 23, 2014).

Moreover, the cases cited by Omni are readily distinguishable. In Adashunas v. Negley, 626 F.2d 600, 603 (7th Cir. 1980), the Seventh Circuit found unascertainable a class of “children entitled to a public education who have learning disabilities and ‘who are not properly identified and/or who are not receiving’ special education.” The court reasoned that “identifying learning disabled children is a gargantuan task,” especially

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

because children who had already been properly identified as learning disabled were excluded from the class. See id. at 603-04. That inquiry bears no relation to the case at hand. And in Stalley v. ADS Alliance Data Systems, Inc., 296 F.R.D. 670, 685-86 (M.D. Fla. 2013), there was evidence that well over a million calls had not been recorded during the class period. Omni’s evidence that some small percentage of unspecified calls were not recorded despite Omni’s policy of recording every incoming call does not approach the scale of unrecorded calls in Stalley. Plaintiffs have defined an ascertainable class and, to the extent Omni argues that “identifying class members” may be difficult, those “concerns are more properly addressed after class certification, except to the extent that they create manageability problems that should be considered under Rule 23(b)(3).” Agne v. Papa John’s Int’l, Inc., 286 F.R.D. 559, 566 (W.D. Wash. 2012).

B. Rule 23(a) Requirements

1. Numerosity

Rule 23(a)(1) requires the class to be so numerous that joinder of individual class members is impracticable. See Fed. R. Civ. P. 23(a)(1). “No exact numerical cut-off is required; rather, the specific facts of each case must be considered. However, numerosity is presumed when where the plaintiff class contains forty or more members.” In re Cooper Cos. Secs. Litig., 254 F.R.D. 628, 634 (S.D. Cal. 2009) (internal citations omitted). Moreover, “it is not necessary to state the exact number of class members when the plaintiff’s allegations plainly suffice to meet the numerosity requirement.” Id. (internal quotation marks omitted). Plaintiffs state that the putative class involves “individuals who collectively placed about 13,000” qualifying calls to Omni during the Class Period. Omni does not contest numerosity, and the allegations “plainly suffice” to meet Rule 23(a)(1).

2. Commonality

Rule 23 also requires the plaintiffs to show that “there are questions of law or fact common to the class.” Fed. R. Civ. P. 23(a)(2). “Commonality requires the plaintiff to demonstrate that the class members have suffered the same injury . . . [and] [t]heir claims must depend upon a common contention . . . of such nature that it is capable of classwide resolution—which means that determination of its truth or falsity will resolve an issue

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

that is central to the validity of each one of the claims in one stroke.” Dukes, 131 S.Ct. at 2551 (internal quotation marks and citations omitted). “What matters to class certification . . . is not the raising of common ‘questions’—even in droves—but, rather the capacity of a classwide proceeding to generate common answers apt to drive the resolution of the litigation.” Id.

The predominance inquiry under Rule 23(b)(3) is “similar to,” but more demanding than, the commonality inquiry under Rule 23(a)(2). See Amchen Prods., Inc. v. Windsor, 521 U.S. 591, 623 n.18 (1997). In other words, a class cannot be certified if common questions of law exist, but are outbalanced by individual questions; conversely, if plaintiffs show predominance, they necessarily show commonality. Omni’s opposition addresses commonality and predominance together and, for efficiency’s sake, the Court does as well in IV.B.1, below.

3. Typicality

Rule 23 next requires that “the claims or defenses of the representative parties” be “typical of the claims or defenses of the class.” Fed. R. Civ. P. 23(a)(2). The purpose of the typicality requirement is to assure that the interest of the named representative aligns with the interests of the class.” Wolin v. Jaguar Land Rover North Am., LLC, 617 F.3d 1168, 1175 (9th Cir. 2010). “The test of typicality ‘is whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct.’” Costco, 657 F.3d at 984 (quoting Hanlon, 976 F.3d at 508)). Thus, typicality is satisfied if the plaintiffs’ claims are “reasonably co-extensive with those of absent class members; they need not be substantially identical.” Hanlon, 150 F.3d at 1020. Where a class representative is subject to unique defenses, typicality may not be satisfied. Hanon v. Dataproducts Corp., 976 F.2d 497, 508 (9th Cir. 1992). The typicality requirement tends to overlap with the commonality and adequacy requirements. See Newberg on Class Actions (Fifth) § 3:30.

Plaintiffs contend that the claims of Ades and Murphy are typical of those of the class because they derive from Omni’s recording of cellular telephone calls without consent. Omni’s opposition brief does not specifically challenge plaintiffs’ showing of typicality, but its “background” section contends that there is insufficient evidence that

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Ades called from a cellular telephone. Plaintiffs respond with deposition testimony explaining that Ades called from a cordless phone plugged into the base station of a Verizon Wireless Home Phone Connect system, and that his call to Omni took place over the Verizon Wireless cellular network.

Ades’s and Murphy’s claims are “reasonably co-extensive” with those of other putative class members. They allege a course of conduct by Omni common to the class, and privacy invasions typical to those of the class generally. Therefore, the typicality requirement is met.

4. Adequacy

The final Rule 23(a) requirement is that “the representative parties will fairly and adequately protect the interests of the class.” Fed. R. Civ. P. 23(a)(4). The adequacy inquiry involves whether “the named plaintiffs and their counsel have any conflicts of interest with other class members” and whether “the named plaintiffs and their counsel will prosecute the action vigorously on behalf of the class.” Hanlon, 150 F.3d at 1020.

Plaintiffs argue that adequacy is met because Ades and Murphy do not have interests antagonistic to those of the class, and because plaintiffs’ counsel have experience with class actions, including ones involving CIPA. Omni contests adequacy on the ground that the putative class action is “attorney-driven and constructed.” Mem. Opp’n Class Cert. at 24. Omni argues that former putative class representative class representative Woolery gave false deposition testimony unchecked by plaintiffs’ counsel, and that the substitution of Murphy for Woolery was procedurally improper.

It does not appear that either Ades or Murphy has interests antagonistic to the class, and plaintiffs have offered evidence that they will prosecute the action vigorously. Moreover, the Court has the authority to authorize a class representative at this stage who was not previously a named plaintiff. See Manual for Complex Litigation (Fourth) § 21.26 (explaining that a district court “may simply designate [the new] person as a representative in the order granting class certification”). Additionally, assuming that Murphy was solicited by counsel, that does not undermine a finding of adequacy. There is nothing inherently improper with the recruitment of class representatives, and where existing named plaintiffs become unavailable or unsuitable, allowing the recruitment of

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

replacements is even recommended. Manual for Complex Litigation (Fourth) § 21.26; In re Vitamin C Antitrust Litigation, 279 F.R.D. 90, 108 (E.D.N.Y. 2012). Moreover, even where solicitation of clients is improper under rules of professional responsibility, denial of class certification is not an appropriate remedy. Busby v. JRHBW Realty, Inc., 513 F.3d 1314, 1324 (11th Cir. 2008). Therefore, plaintiffs have established adequacy.

C. Rule 23(b)(3) Requirements

Under Rule 23(b)(3), class certification is appropriate “if Rule 23(a) is satisfied” and if “the court finds that [1] the questions of law or fact common to class members predominate over any questions affecting only individual members, and that [2] a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.” Fed. R. Civ. P. 23(b)(3); Local Joint Exec. Bd. of Culinary/Bartender Trust Fund v. Las Vegas Sands, Inc., 244 F.3d 1152, 1162–63 (9th Cir. 2001). A class proponent carries the burden of showing compliance with Rule 23(b)(3) “through evidentiary proof.” Comcast, 133 S.Ct. at 1432.

1. Predominance

The predominance inquiry “trains on legal or factual questions that qualify each class member’s case as a genuine controversy.” Amchem Prods, Inc. v. Windsor, 521 U.S. 591, 625 (1997). “When one or more of the central issues in the action are common to the class and can be said to predominate,” a class action will be considered proper “even though other matters will have to be tried separately.” Gartin v. S&M NuTec LLC, 245 F.R.D. 429, 435 (C.D. Cal. 2007). “Because no precise test can determine whether common issues predominate, the Court must pragmatically assess the entire action and the issues involved.” Romero v. Producers Dairy Foods, Inc., 235 F.R.D. 474, 489 (E.D. Cal. 2006). “Implicit in the satisfaction of the predominance test is the notion that the adjudication of common issues will help achieve judicial economy.” Valentino v. Carter-Wallace, Inc., 97 F.3d 1227, 1234 (9th Cir. 1996). The focus is on whether the proposed class is “sufficiently cohesive to warrant adjudication by representation.” Amchem Prods., 521 U.S. at 623.

In support of commonality and predominance, plaintiffs assert that common questions include “(1) whether Omni had a policy and practice of recording calls to the

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Contact Center; (2) whether Omni had a policy and practice of advising callers that telephone calls are recorded; (3) whether the callers consented to the recording; and (4) the monetary and injunctive remedies to which class members are entitled.” Mem. Supp. Class Cert. at 20-21. Plaintiffs argue that classwide evidence can establish a *prima facie* case that the calls were recorded, that class members were not warned of recording, and that class members did not consent to the recording.

Omni asserts that two types of individual issues will predominate. First, Omni argues that plaintiffs cannot prove on a classwide basis the “injury” required to bring a damages action under § 637.2 because some putative class members assumed their calls would be recorded, and therefore suffered no harm from being recorded without warning. But as explained more fully in the Court’s order denying Omni’s motion for summary judgment, the only “harm” required by § 637.2 “is the unauthorized recording.” California Practice Guide: Civil Procedure Before Trial Claims & Defenses § 4:1690; see In re Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784, at *65-67 (N.D. Cal. Sep. 26, 2013) (rejecting an argument that § 632.7 requires independent injury aside from an invasion of statutory CIPA rights); Lieberman v. KCOP Television, Inc., 110 Cal. App. 4th 156, 167 (2003) (“[A]n actionable violation of section 632 occurs the moment the surreptitious recording is made.”).

Next, Omni contends that the question of implied consent to recording will require individualized inquiries.⁴ In support, Omni cites (1) declarations of putative class

⁴It is unclear whether § 632.7 places the burden of showing consent or a lack thereof on plaintiffs or defendants, and the Court did not find a case addressing the issue in the CIPA context. On the one hand, the California Advisory Committee’s jury instructions on § 632.7 require a plaintiff to show that a defendant “did not have consent of all parties to the conversation.” Judicial Council of California Civil Jury Instruction 1809. On the other hand, at least some cases interpreting similar federal privacy statutes—which both parties cite as instructive on consent issues—seem to place the burden on the defendant. See, e.g., In re Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003) (“We think, at least for the consent exception under the [Electronic Communications Privacy Act] in civil cases, that it makes more sense to place the burden of showing consent on the party seeking the benefit of the exception, and so hold.”); In re Yahoo Mail Litig., No.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

members indicating an expectation that calls to Omni or similar companies would be recorded; (2) requests by putative class members that recordings of prior calls be accessed, suggesting awareness that those calls were recorded; and (3) a survey concluding that half of California residents who called “business class or luxury hotels” within a recent one-year period assumed their calls were recorded.

Plaintiffs criticize Omni’s conceptualization of and evidence of implied consent. Plaintiffs deny that any of the three declarants cited are class members, and argue that regardless, the declarations do not show consent prior to recording. They argue that Omni has not shown that any request to access prior recordings was made by a class member, and that in any event such a request would not show consent, which requires “at a minimum . . . evidence that the class member had actual knowledge that Omni was recording the call.” Mem. Supp. Class Cert. at 15. Finally, plaintiffs criticize the study on several grounds. First, they argue that it tested expectations, not consent. Second, they contend that the studied population does not correspond to the class because the survey asked about a time period beginning several months after the close of the Class Period. In the interim, plaintiffs argue, Omni began warning all callers of monitoring and recording, and similar hotels may also have changed their policies. Finally, plaintiffs attack the sampling methodology and phrasing of Omni’s survey.

Omni relies heavily on a single sentence from Torres v. Nutrisystem, Inc., 289 F.R.D. 587 (C.D. Cal. 2013). In that case, denying a class certification pursuant to § 632.7 of callers who had bypassed an automated recording disclosure, the district court stated that “callers who never heard the Disclosure, but actually expected the calls to be recorded, may have impliedly consented to the recording by the very act of making the

5:13-cv-04980, 2014 WL 3962824, at *7, — F. Supp. 2d — (N.D. Cal. Aug. 12, 2014) (similar). Either way, the Court notes that plaintiffs have put forth undisputed evidence that Omni did not notify putative class members that they would be recorded at the outset of the calls at issue. Further, whether or not consent is an affirmative defense, the issue for purposes of predominance remains whether the evidence shows that individual inquiries into consent will dominate the trial. Cf. Waste Mgmt. Holdings, Inc. v. Mowbray, 208 F.3d 288, 295 (1st Cir. 2000) (stating that “affirmative defenses should be considered in making class certification decisions”).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

call.” *Id.* at 595. But the Court finds more persuasive a more detailed analysis by the California Supreme Court in *Kearney* of § 632, which contains the identical “without the consent of all parties” language as § 632.7. In that case, the court explained:

As made clear by the terms of section 632 as a whole, this provision does not absolutely preclude a party to a telephone conversation from recording the conversation, but rather simply prohibits such a party from secretly or surreptitiously recording the conversation, *that is, from recording the conversation without first informing all parties to the conversation that the conversation is being recorded.* If, after being so advised, another party does not wish to participate in the conversation, he or she may simply decline to continue the communication. A business that *adequately advises all parties to a telephone call, at the outset of the conversation,* of its intent to record the call would not violate the provision.

Kearney, 39 Cal. 4th at 117-118 (emphasis added). In a footnote, the Supreme Court also criticized the precise argument Omni makes here:

[T]he Court of Appeal suggested that even in the absence of an explicit advisement, clients or customers of financial brokers such as SSB “know or have reason to know” that their telephone calls with the brokers are being recorded. The Court of Appeal, however, did not cite anything in the record or any authority establishing such a proposition as a matter of law, and in light of the circumstance that California consumers are accustomed to being informed at the outset of a telephone call whenever a business entity intends to record the call, it appears equally plausible that, in the absence of such an advisement, a California consumer reasonably would anticipate that such a telephone call is not being recorded

Id. at 118 n.10. Thus, the Court does not find that evidence that some class members *expected* their calls to be recorded raises predominant issues of consent in the absence of any evidence that Omni—or anyone else—ever notified callers that Omni would record their calls before or at the outset of any call.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Omni argues that individual issues of consent will predominate even in the absence of any prior notice, because consent “is an intensely factual question” that “requires looking at all of the circumstances . . . to determine whether an individual knew that her communications were being intercepted.” In re Google, Inc. Gmail Litig., No. 13-MD-02430, 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014). But Omni cites no case in which a class was rejected on consent grounds despite the absence of any evidence of advance notice. Despite extensive discovery, Omni has not produced evidence that a single person meeting the class definition actually consented to a call being recorded during the Class Period.⁵ Nor does the Court find the declarations of Omni’s employees or the Zauberman study sufficient to show that individual consent issues will predominate. As the Ninth Circuit stated in a Title III wiretapping case cited by Omni, “foreseeability of monitoring is insufficient to infer consent.” United States v. Staves, 383 F.3d 977, 981 (9th Cir. 2004).⁶ Thus, that unidentified callers sometimes

⁵This statement does not depend on the fact that plaintiffs have narrowed their proposed class definition since the First Amended Complaint. Even if all three declarants did fit the class definition, their evidence would only indicate that they anticipated that they might have been recorded and were not aggrieved to find out that they were—not that they actually consented at the time of the call.

⁶At oral argument, Omni submitted that the Court ignores the next sentence of Staves: “Rather, the circumstances must indicate that a party to the communication knew that interception was likely and agreed to the monitoring.” 383 F.3d at 981. Omni has not produced evidence that any class members “agreed to the monitoring.” Moreover, the parenthetical to that sentence’s citation reads, “inferring knowing agreement to monitoring of prison telephone conversations *where the defendant received several warnings of the monitoring.*” Id. (emphasis added)). In the case described by that parenthetical, United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1996), a law enforcement agency had “posted signs above the phones warning of the monitoring and taping. Furthermore, Van Pock signed a consent form and was also given a prison manual a few days after his arrival.” The Van Poyck court also cited a previous case in which consent was inferred where the caller “(1) had attended a lecture discussing the taping procedure; (2) had been given a copy of the Inmate Information Handbook discussing the procedure; (3) had seen notices posted on telephones; and (4) had signed a

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

asked for previous calls to be accessed, suggesting that they thought those calls might have been recorded, does not show that evidence of individual consent to recording will dominate the trial. Nor does Omni’s study, even ignoring plaintiffs’ methodological criticisms, show that any individual class members actually consented at the time to their calls being recorded by Omni.

Thus, unlike in the cases Omni cites, there is no indication that individual consent issues will overwhelm issues plaintiffs have shown to be resolvable through classwide proof. Compare In re Google, Inc. Gmail Litig., 2014 WL 1102660, at *17-18 (finding that individual inquiries into consent would be necessary where Google pointed out that putative class members could have learned of Google’s email scanning from various Google and third-party service provider disclosures as well as widespread media coverage of Google’s scanning practices), and Nutrisystem, 289 F.R.D. at 595 (many putative class members had likely heard a disclosure of recording on a prior call before bypassing the disclosure on a subsequent call), with Silbaugh v. Viking Mag. Servs., 278 F.R.D. 389, 393 (N.D. Ill. 2012) (“Having produced no evidence that any individual consented to receive the text messages . . . defendant is unable to realistically argue that individual issues regarding consent outweigh the commonality.”). Moreover, Omni “is in the best position to come forward with evidence of individual consent and will not be precluded from presenting admissible evidence of individual consent if and when individual class members are permitted to present claims.” Agne v. Papa John’s Int’l, Inc., 286 F.R.D. 559, 570 (W.D. Wash. 2012). The Court can of course reconsider the propriety of class adjudication at a later juncture if such evidence comes to light.

Therefore, on the record before it, the Court finds that plaintiffs have met their burden of showing that common questions will predominate at trial.

form consenting to the procedure.” Id. (citing United States v. Amen, 831 F.2d 373, 379 (2d Cir. 1987)). Here, as stated above, Omni has presented no evidence that a single caller received a single warning of monitoring or recording. A detailed examination of Staves therefore provides even more support for plaintiffs’ position.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

2. Superiority

Rule 23(b)(3) sets forth four relevant factors for determining whether a class action is “superior to other available methods for the fair and efficient adjudication of the controversy.” Fed. R. Civ. P. 23(b)(3). These factors include:

- (A) the class members’ interests in individually controlling the prosecution or defense of separate actions;
- (B) the extent and nature of any litigation concerning the controversy already begun by or against class members;
- (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and
- (D) the likely difficulties in managing a class action.

Id.

“[C]onsideration of these factors requires the court to focus on the efficiency and economy elements of the class action so that cases allowed under subdivision (b)(3) are those that can be adjudicated most profitably on a representative basis.” Zinser v. Accufix Research Inst., Inc., 253 F.3d 1180, 1190 (9th Cir. 2001) (internal quotation marks and citation omitted), amended by 273 F.3d 1266 (9th Cir. 2001). District courts may also consider “other, non-listed factors,” as the Ninth Circuit has recently reiterated:

Superiority must be looked at from the point of view (1) of the judicial system, (2) of the potential class members, (3) of the present plaintiff, (4) of the attorneys for the litigants, (5) of the public at large, and (6) of the defendant. The listing is not necessarily in order of importance . . . Superiority must also be looked at from the point of view of the issues.”

Bateman v. Am. Multi-Cinema, Inc., 623 F.3d 708, 713 (9th Cir. 2010) (quoting Kamm v. Cal City Dev. Co., 509 F.2d 205, 212 (9th Cir. 1975)).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

Plaintiffs submit that a class action is superior because the only alternative would be “thousands of separate cases litigated from start to finish.” Mem. Supp. Class Cert. at 24. Moreover, they assert that available damages are insufficient to incentivize individual litigation, that there is no evidence of existing litigation involving the same claims or parties, and that the Central District is not an undesirable forum. Finally, plaintiffs contend that a class action will be manageable because the key evidence can be presented through a relatively small number of witnesses and, to the extent Omni has admissible evidence that certain calls were not recorded or were consented to, Omni can present that evidence in its defense. Omni responds that adequate incentives exist for individual lawsuits in the form of CIPA’s minimum damages of \$5,000. Moreover, Omni argues that, when aggregated on a classwide basis, CIPA’s damages would be grossly excessive as to violate the Due Process Clause. Plaintiffs respond that under Bateman, consideration of “excessive” statutory damages is improper at the class certification stage. See 623 F.3d at 708.

The Ninth Circuit in Bateman “reserve[d] judgment . . . on whether Rule 23(b)(3) *per se* prohibits consideration of a defendant’s potential liability in deciding whether to certify a class.” 623 F.3d at 713 n.3. Nevertheless, the Court finds sufficient similarities between Bateman and this case to decline to consider allegedly excessive damages as weighing against superiority. Bateman involved a putative class action brought under the Fair and Accurate Credit Transactions Act (FACTA), a federal statute that, like CIPA, provides for statutory damages upon proof of a privacy violation, without evidence of actual damages. Id. at 717-18. The court noted that while many district courts, including several within the Ninth Circuit, had found potential liability a proper superiority consideration, the only federal court of appeals to have addressed the issue with regard to a similar damages provision had held such consideration improper. Id. at 715 (discussing Murray v. GMAC Mortg. Corp., 434 F.3d 948 (7th Cir. 2006)). The Ninth Circuit then analyzed FACTA to determine whether denial of class certification on excessive aggregated damages grounds would be consistent with congressional intent. Bateman, 623 F.3d at 716-21. The court noted that Congress, despite being aware of the availability of the class action form, did not cap or otherwise limit damages that could be obtained in class actions, as it had for other statutes. Id. at 718, 720. The court reasoned Congress had decided that the penalties it set served compensatory and deterrence functions and were proportionate to the prohibited conduct. Id. at 719. The court then stated that this “proportionality does not change as more plaintiffs seek relief” and

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

concluded that it was “not appropriate to use procedural devices to undermine laws of which a judge disapproves.” Id. (citing Murray, 434 F.3d at 954); see also In re Napster, Inc. Copyright Litig., No. C MDL-00-1369 MHP, 2005 WL 1287611, at *11 (N.D. Cal. June 1, 2005) (“[T]he conclusion that class action treatment might somehow influence the proportionality of a statutory damages award is logically flawed.”). Accordingly, the unanimous panel held that the district court had abused its discretion by “considering the proportionality of the potential liability to the actual harm alleged in its Rule 23(b)(3) superiority analysis.” Bateman, 623 F.3d at 721.

Here, the Legislature evidently decided that minimum damages of \$5,000 per violation serve CIPA’s purposes and are proportional to the harm caused by CIPA violations. Plaintiffs’ action is not the first class action to be filed under § 637.2, and the Legislature could have acted to limit damages in response to any concerns about the liability sought in previous class actions. Cf. Agne v. Papa John’s Int’l, Inc., 286 F.R.D. 559, 572 (W.D. Wash. 2012) (concluding that Bateman’s reasoning “applies with equal force” to a putative class action seeking statutory damages under the Telephone Consumer Protection Act). Moreover, for reasons more fully explained in the order denying Omni’s motion for summary judgment, issues of excessive damages are better addressed at a later stage of the litigation. See Murray, 434 F.3d at 954 (“An award that would be unconstitutionally excessive may be reduced, but constitutional limits are best applied after a class has been certified.”). Finally, the Court is not persuaded that \$5,000 in damages is so clearly sufficient to motivate individual litigation involving complex factual and legal issues as to weigh against class certification.

Therefore, the Court finds that plaintiffs have satisfied their burden of showing superiority.

V. CONCLUSION

For the foregoing reasons, plaintiffs’ motion for class certification is GRANTED. The following class is certified:

All individuals who, between March 15, 2012 and March 22, 2013, inclusive, while physically present in California, participated in a telephone call with a live representative of Omni that was: (1) placed

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-cv-02468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES & HART WOOLERY v. OMNI HOTELS MANAGEMENT CORPORATION, ET AL.		

to one of the following Omni numbers: (888) 444-6664, (800) 843-6664, (877) 440-6664, (800) 788-6664, or (800) 809-6664; (2) made from a telephone number that includes a California area code (*i.e.*, 209, 213, 310, 323, 408, 415, 424, 442, 510, 530, 559, 562, 619, 626, 650, 657, 661, 669, 707, 714, 747, 760, 805, 818, 831, 858, 909, 916, 925, 949, or 951); and (3) transmitted via cellular telephone on the network of AT&T, Verizon Wireless, or Sprint. The class excludes all employees of defendant and plaintiffs' counsel and their employees.

The Court appoints as class counsel the Law Office of Zev B. Zysman, A Professional Corporation, and Dostart Clapp & Coveney, LLP.

IT IS SO ORDERED.

Initials of Preparer

00 : 16

CMJ

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Present: The Honorable	CHRISTINA A. SNYDER	
Catherine Jeang	Laura Elias	N/A
Deputy Clerk	Court Reporter / Recorder	Tape No.
Attorneys Present for Plaintiffs:		Attorneys Present for Defendants:
James Hannink		Angela Agrusa
James Clapp		
Zev Zysman		
Proceedings:	DEFENDANT’S MOTION FOR SUMMARY JUDGMENT PURSUANT TO FEDERAL RULE OF CIVIL PROCEDURE 56	

I. INTRODUCTION

Plaintiffs Steven Ades (“Ades”) and Hart Woolery (“Woolery”) filed the instant putative class action on March 15, 2013 in Los Angeles County Superior Court. Defendant in this action is Omni Hotels Management Corporation (“Omni”). Omni removed the case to this Court based on diversity of citizenship on April 8, 2013. Dkt. #1. Plaintiffs have since sought to substitute Jonathan Murphy (“Murphy”) for Woolery as class representative. Dkt. #55, 59.

On April 29, 2013, plaintiffs filed the First Amended Complaint (“FAC”). The FAC asserts claims for relief pursuant to the California Invasion of Privacy Act (“CIPA”), California Penal Code § 630 *et seq.* In brief, these claims assert that plaintiffs called Omni’s toll-free telephone numbers and provided Omni representatives with personal information. FAC ¶¶ 16 – 17. Plaintiffs allege that when they placed their calls to Omni’s toll-free telephone numbers, they were not apprised that the call might be recorded. *Id.* Plaintiffs further allege that Omni has a company-wide policy of recording inbound telephone conversations with consumers without seeking permission or informing consumers about the monitoring. *Id.* ¶¶ 18 – 19.

Omni filed a motion for summary judgment on July 30, 2014, Dkt. #63, and a corrected memorandum of points and authorities in support thereof on August 1, 2014,

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Dkt. #65. Plaintiffs filed an opposition on August 18, 2014. Dkt. #67. Omni replied on August 28, 2014. Dkt. #72. The parties appeared at oral argument on September 8, 2014. After considering the parties’ arguments, the Court finds and concludes as follows.

II. BACKGROUND¹

Plaintiffs brought this suit on behalf of themselves and “[a]ll individuals who, between March 15, 2012 and March 22, 2013, inclusive (the ‘Class Period’), while physically present in California, participated in a telephone call with a live representative of Omni” that was placed to one of several Omni toll-free numbers, made from a telephone number with a California area code, and transmitted via the AT&T, Verizon Wireless, or Sprint cellular telephone networks. Dkt. #59. Plaintiffs contend that they called Omni’s toll-free phone number and, without being warned that their calls were being recorded, provided Omni representatives with personal information including their names, phone numbers, e-mail addresses, and credit card numbers and expiration dates. FAC ¶¶ 16-17. Plaintiffs allege that unwarned and unconsented recording and monitoring of inbound calls pursuant to Omni company policy violated § 632.7 of CIPA, entitling them to statutory damages. *Id.* ¶¶ 31-46. The calls at issue were placed to an Omni call center located in Omaha, Nebraska. Defendant’s Statement of Uncontroverted Facts (“DSUF”) ¶¶ 1-2; Plaintiff’s Statement of Disputes of Material Fact (“PSDMF”) ¶¶ 1-2.

Omni states that all relevant incoming calls were recorded solely for quality assurance purposes. DSUF ¶¶ 2, 4. While disputing that this is relevant to the motion for summary judgment, plaintiffs cite evidence that the recordings were also made so that Omni personnel could consult them in the event of a dispute between Omni and a customer. PSDMF ¶¶ 2, 4. Omni contends that, at all times relevant to this motion, it neither had nor has the ability to “identify an incoming cellular caller’s location or state residency.” DSUF ¶ 5. Plaintiff denies this, and argues that Omni could identify the origin of calls by (1) retaining a “location information services company to provide Omni with real-time data . . . indicating the originating cell tower location; (2) utilizing an

¹The facts set forth in this section are not all undisputed and are provided for background purposes only.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

“Integrated Voice Response” system that would ask callers to indicate by pressing a keypad button whether they were calling from California; (3) instructing its agents to ask whether customers are calling from California; or (4) using the caller’s area code as a “reasonable proxy for geographic location.” PSDMF ¶¶ 5, 6. Since the filing of this lawsuit, Omni has implemented an automated notification stating that calls to the Omaha call center may be recorded. PSDMF ¶ 13.

III. LEGAL STANDARD

Summary judgment is appropriate where “there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). The moving party bears the initial burden of identifying relevant portions of the record that demonstrate the absence of a fact or facts necessary for one or more essential elements of each claim upon which the moving party seeks judgment. See Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986).

If the moving party meets its initial burden, the opposing party must then set out specific facts showing a genuine issue for trial in order to defeat the motion. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 250 (1986); see also Fed. R. Civ. P. 56(c), (e). The nonmoving party must not simply rely on the pleadings and must do more than make “conclusory allegations [in] an affidavit.” Lujan v. Nat’l Wildlife Fed’n, 497 U.S. 871, 888 (1990); see also Celotex, 477 U.S. at 324. Summary judgment must be granted for the moving party if the nonmoving party “fails to make a showing sufficient to establish the existence of an element essential to that party’s case, and on which that party will bear the burden of proof at trial.” Id. at 322; see also Abromson v. Am. Pac. Corp., 114 F.3d 898, 902 (9th Cir. 1997).

In light of the facts presented by the nonmoving party, along with any undisputed facts, the Court must decide whether the moving party is entitled to judgment as a matter of law. See T.W. Elec. Serv., Inc. v. Pac. Elec. Contractors Ass’n, 809 F.2d 626, 631 & n.3 (9th Cir. 1987). When deciding a motion for summary judgment, “the inferences to be drawn from the underlying facts . . . must be viewed in the light most favorable to the party opposing the motion.” Matsushita Elec. Indus. Co. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986) (citation omitted); Valley Nat’l Bank of Ariz. v. A.E. Rouse & Co., 121 F.3d 1332, 1335 (9th Cir. 1997). Summary judgment for the moving party is proper

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

when a rational trier of fact would not be able to find for the nonmoving party on the claims at issue. See Matsushita, 475 U.S. at 587.

IV. DISCUSSION

Omni advances five arguments in support of its motion. First, it argues that Nebraska law, not California law, governs Omni’s conduct. Second, it maintains that if § 632.7 is imposed on Omni’s national call center as plaintiffs urge, it would violate the dormant Commerce Clause of the federal Constitution. Third, Omni contends that the statutory damages sought by plaintiffs violate the Excessive Fines Clause of the federal Constitution and the due process guarantees of the California and federal constitutions. Fourth, it argues that § 632.7 does not apply to call participants. Finally, Omni denies that plaintiffs have been “injured” as required to bring a damages claim under § 632.7. Each argument is addressed in turn.

A. Choice of Law

“Federal courts sitting in diversity jurisdiction look to the law of the forum state in choice-of-law determinations.” Fields v. Legacy Health Sys., 413 F.3d 943, 950 (9th Cir. 2005). California applies a three-step “government interest” test to choice-of-law issues, which the state’s Supreme Court has articulated as follows:

First, the court determines whether the relevant law of each of the potentially affected jurisdictions with regard to the particular issue in question is the same or different. Second, if there is a difference, the court examines each jurisdiction's interest in the application of its own law under the circumstances of the particular case to determine whether a true conflict exists. Third, if the court finds that there is a true conflict, it carefully evaluates and compares the nature and strength of the interest of each jurisdiction in the application of its own law “to determine which state's interest would be more impaired if its policy were subordinated to the policy of the other state,” and then ultimately applies the law of the state whose interest would be the more impaired if its law were not applied.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Kearney v. Salomon Smith Barney, Inc., 39 Cal. 4th 95, 107-08 (1996) (internal quotation marks omitted). Omni makes two arguments concerning the applicable law.

1. Difference Between California and Nebraska Law

First, Omni argues that the relevant California and Nebraska laws do not differ because both states exempt service monitoring from the applicable privacy statutes. Therefore, Omni contends, the Court need not advance past the first step of the government interest analysis.

When construing a state statute, federal courts apply state law of statutory construction. Bass v. County of Butte, 458 F.3d 978, 981 (9th Cir. 2006). Under California law, a court’s “fundamental task . . . is to determine the Legislature’s intent so as to effectuate the law’s purpose.” People v. Murphy, 25 Cal. 4th 136, 142 (2001). This task begins with the plain meaning of the statutory text considered in the context of “the entire substance of the statute in order to determine the scope and purpose of the provision.” Id. Legislative history should only be considered where the statutory text is ambiguous. Kaufman & Broad Communities, Inc. v. Performance Plastering, Inc., 133 Cal. App. 4th 26, 29 (2005) (“Our role in construing a statute is to ascertain the Legislature’s intent so as to effectuate the purpose of the law. In determining intent, we look first to the words of the statute, giving the language its usual, ordinary meaning. If there is no ambiguity in the language, we presume the Legislature meant what it said, and the plain meaning of the statute governs.”). Additionally, where consideration of legislative history is appropriate, “legislative history must shed light on the collegial view of the Legislature *as a whole*.” Id. at 30 (emphasis in original).

In support of its contention that the two states exempt service monitoring, Omni cites passages from CIPA’s legislative history and changes to the California Public Utilities Commission’s (“the PUC”) regulation of the telephone industry. Most of Omni’s arguments and supporting citations were raised on Omni’s motion to dismiss, Dkt. #12, as set forth and rejected in the Court’s prior order, Dkt. #17. That order, however, reserved the question of the “applicability and scope of the Public Utility Exemption” that Omni claims applies. Id. at 7.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

To its arguments raised on the motion to dismiss, Omni adds more detail regarding the PUC’s regulation of the telephone industry. Under General Order 107-B, the PUC formerly required telephone utilities to file tariffs setting conditions for use of its networks by companies that provided their own terminal equipment and monitored or recorded conversations between their employees and customers.² Def.’s Request for Judicial Notice Ex. F at 12. Omni reasons that because CIPA exempts from liability the use of “instruments, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility,” Cal. Pen. Code § 632.7(b)(2), service observing was excluded from CIPA’s coverage by the “public utility exception.” The PUC recently began allowing utility companies to “de-tariff” so that they would no longer have to file tariffs, including those required under General Order 107-B. Omni argues that the PUC’s relaxation of service reporting requirements “cannot rewrite CIPA and turn service observing from an honored practice into a crime.”³ Mem. Supp. Mot. Summ. J. at 5.

Omni does not claim that any recordings made during the Class Period were literally made on equipment “furnished and used pursuant to the tariffs of a public utility.” Cal. Pen. Code § 632.7(b)(2). The text of § 632.7(b)(2) suggests that the public utilities exception itself does not apply unless this condition is met; moreover, the California Supreme Court has declined to apply the exception where “there indeed was no tariff” applicable “at the time of the conduct alleged.” Ribas v. Clark, 38 Cal. 3d 355, 362 (1985); see also Bales v. Sierra Trading Post, Inc., No. 13-cv-1894 JM(KSC), 2013

²A “tariff” filed with the PUC “consists of schedules showing all rates, tolls, rentals, charges, and classifications collected or enforced, or to be collected or enforced, together with all rules, contracts, privileges, and facilities which in any manner affect or relate to rates, tolls, rentals, classifications, or service.” Cal. Pub. Util. Code § 489.

³However, adjacent provisions of the same PUC order cited by Omni state that customers who provide their own terminal equipment must provide notice of any monitoring or recording. Def.’s Request for Judicial Notice Ex. F at 12. This order explained that the tariff conditions for such companies were intended “to assure the same degree of privacy” for these telephone conversations. Id. Similarly, all of the no-longer-filed carrier tariffs cited by Omni included provisions requiring notice of recording or monitoring. See id. Ex. G at 3; id. Ex. H at 4; id. Ex. I at 12.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

U.S. Dist. LEXIS 170443, at *11 (S.D. Cal. Dec. 3, 2013) (denying a motion to dismiss on public utility exception grounds where the defendant could not proffer that its recording equipment was furnished and used pursuant to a published tariff).

Rather, Omni argues that because the PUC once regulated monitoring and recording of the kind at issue here, § 632.7 should be read as if it never applied to service monitoring. Most courts considering § 632.7 or the identical exception in § 632(e), however, have rejected this argument. See, e.g., Kight v. CashCall, Inc., 200 Cal. App. 4th 1377, 1391 (2011) (holding that § 632 “contains no exceptions applicable when a business monitors a telephone conversation even if the monitoring is for a legitimate business purpose”); Bales, 2013 U.S. Dist. LEXIS 170443, at *11 (declining to read a “service-observing” exception into § 632(e)); Nader v. Capital One Bank (USA), N.A., cv-12-1265-DSF (RZx), slip op. at 5-6 (C.D. Cal. June 11, 2013) (deeming “meritless” a similar argument for a customer service exemption); Dake v. Receivables Performance Mgmt., LLC, No. 12-cv-1680-VAP (SPx), 2013 U.S. Dist. LEXIS 160341, at *13 (C.D. Cal. April 16, 2013) (“Neither Section 632 nor 632.7 contains an exception for service monitoring. The language of these sections is unambiguous.”); Knell v. FIA Card Servs., N.A., No. 12-cv-0426-AJB (WVG), 2013 U.S. Dist. LEXIS 187551, at *23 (S.D. Cal. Feb. 21, 2013) (“Section 632(e) does not create a ‘service-observing exemption in its unambiguous provisions and, thus, the Court declines to create one based upon the statute’s legislative history.”); Zephyr v. Saxon Mortg. Servs., 873 F. Supp. 2d 1223, 1231 (E.D. Cal. 2012) (“[B]oth 632 and 632.7 are unambiguous and broad in the scope of their protection: together[,] they prohibit ‘[e]very person’ from recording any confidential communication, including telephone calls. . . . If there was any doubt about whether the statute clearly and unambiguously covered [business telephone monitoring], the Kearney decision dispelled it.”).

Omni attempts to ignore authorities rejecting a service monitoring exception by reasoning that “the courts that have actually addressed CIPA’s legislative history have concluded that CIPA does not apply to service observing.” Mem. Supp. Mot. Summ. J. at 6. But because the statute’s meaning is plain and unambiguous, examination of the legislative history is improper. See Kaufmann, 133 Cal. App. 4th at 29 (“If there is no ambiguity in the language, we presume the Legislature meant what it said, and the plain meaning of the statute governs.”). Omni also attempts to cast doubt on plaintiffs’ cited cases because they were decided before the recent opinion of the “*only* Ninth Circuit

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

jurist to consider the import of the Public Utility Exemption.” Mem. Supp. Mot. Summ. J. at 6 (emphasis in original) (citing Young v. Hilton Worldwide, Inc., No. cv-12-56189, 2014 WL 1087777 (9th Cir. Mar. 20, 2014) (Mozt, J., dissenting)). Although supportive of Omni’s position, this dissenting opinion of a senior district judge sitting by designation does not persuade the Court to ignore the weight of authority on this point.

Omni cites some cases supporting a service monitoring exemption; however, the Court finds them less persuasive than those discussed above. The court in Shin v. Digi-Key Corp., No. cv-12-5415 PA (JCGx), 2012 WL 5503847, at *3 (C.D. Cal. Sep. 17, 2012), for example, mostly based its ruling on the ground that the plaintiff’s call was not a “confidential communication” pursuant to § 632, a consideration not applicable with regard to § 632.7.⁴ Moreover, in deciding that legislative history “further supported” its holding, the Shin court did not have the benefit of the later-decided cases cited above. The principal case relied upon by the Shin court was Sajfr v. BBG Communications, Inc., No. 10-cv-2341 AJB (NLS), 2012 WL 398991 (S.D. Cal. Jan. 10, 2012). In that case, the district court determined that it lacked subject matter jurisdiction because no conduct was alleged to have taken place in California, and added as an “additional argument” that “the legislative history of § 632 reflects that it was not intended to prohibit ‘service-observing’ because the legislature deemed that practice to be in the public’s best interest.” Id. at *5. The same district judge to decide Sajfr, however, found in a later case that reliance on the same “legislative history [was] misplaced as the statutory language is clear and unambiguous,” and explicitly stated that § 632 “does not create a ‘service-observing’ exemption.” Knell, 2013 U.S. Dist. LEXIS 187551, at *23.⁵

⁴See Brown v. Defender Security Comp., No. cv-12-7319-CAS (PJWx), 2012 WL 5308964 (C.D. Cal. Oct. 22, 2012) (finding that § 632.7, unlike § 632, is not limited to confidential communications); see also Flanagan v. Flanagan, 27 Cal. 4th 766, 771 n.2 (2002) (“Section 632.7 . . . applies to all communications, not just confidential communications.”).

⁵Omni also cites two Los Angeles County Superior Court orders finding a service monitoring exemption, only one of which is a written opinion. See Mem. Supp. Summ. J. at 7. The Superior Court has reached the opposite conclusion in a pair of recent opinions. See Newport v. BPG Home Warranty Co., No. BC488142, slip op. at 9 (L.A. Cnty. Sup.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Based on the foregoing, the Court finds (1) that the statutory public utility exemption does not apply to Omni’s conduct and (2) that CIPA does not contain a broad exception for routine service monitoring. Accordingly, the Court rejects Omni’s argument that CIPA does not differ from Nebraska law in relevant respects.

2. Remaining Government Interest Analysis

Omni argues in the alternative that if there is a conflict between California and Nebraska law—that is, if § 632.7 makes illegal non-consensual recordings made for service monitoring purposes—Nebraska’s interests in applying its law outweigh those of California. Nebraska law permits employers to “intercept, disclose, or use” communications related to “any activity which is a necessary incident to the rendition of . . . [its] service or to the protection of the rights or property of the carrier or provider of such communication services.” Neb. Rev. Stat. § 86-920(2)(a). Based on this provision, Omni contends that Nebraska favors allowing businesses to monitor their employees, as to provide better customer service, over protecting consumer privacy directly. Omni argues that the difference in law reflects Nebraska’s attempt to make its state more business-friendly. Moreover, Omni argues that Nebraska law applies because the alleged wrong took place in Nebraska, the location of “the last event necessary to make the actor liable.” Mem. Supp. Summ. J. at 9-10 (citing Mazza v. Am. Honda Motor Co., 666 F.3d 581, 593 (9th Cir. 2012)). Finally—and somewhat in tension with Omni’s premise that, for purposes of this part of the conflict analysis, there is an “irreconcilable conflict” between the two laws—Omni argues that application of Nebraska law would not impair California’s interests because California has expressly embraced service observing as an exception from CIPA.

Ct. May 8, 2013) (Pl.’s Request Judicial Notice Ex. 2) (“Defendant’s attempt to shoehorn its alleged unregulated practice of audio recording into the framework of an exception that was clearly grounded in a heavily regulated world of yesteryear is unavailing.”); Zamar v. Mercury Ins. Co., No. BC469266, slip op. at 5 (L.A. Cnty. Sup. Ct., Apr. 17, 2013) (Pl.’s Request Judicial Notice Ex.1) (“The legislative history, however, is irrelevant here.”).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Plaintiffs first respond that Kearney, which involved CIPA and Georgia’s single-consent recording law, is dispositive of the choice of law issue. Second, they dispute Omni’s characterization of Nebraska as a “zero-consent” state as regards service monitoring, pointing out that the statute cited by Omni provides: “employers and providers shall not utilize service observing or random monitoring except for mechanical, service quality, or performance control checks as long as reasonable notice of the policy of random monitoring is provided to their employees.” Neb. Rev. Stat. § 86-290(2)(a). Next, they argue that California’s interests in its residents’ privacy would be significantly impaired by the application of Nebraska law because Californians’ privacy would only be protected when they placed calls to businesses also located in California. Moreover, they argue that allowing out-of-state companies (but not California companies) to utilize undisclosed recordings would advantage out-of-state companies at in-state companies’ and California residents’ expense. Finally, again citing Kearney, 39 Cal. 4th at 126-27, plaintiffs argue that Nebraska’s interests would not be significantly impaired by the application of California law because California is more protective of privacy interests than Nebraska and neither Nebraska law nor cited business reasons require the secret recording of customer service calls.

In Kearney, plaintiffs alleged that Atlanta-based employees of a nationwide brokerage firm had repeatedly “recorded telephone conversations with California clients without the clients’ knowledge or consent.” 39 Cal. 4th at 99. The California Supreme Court first held that a true conflict existed between § 632 and Georgia privacy law. Id. at 100. The court then found that “the failure to apply California law in this context would impair California’s interest in protecting the degree of privacy afforded to California residents by California law more severely than the application of California law would impair any interests of the State of Georgia.” Id. The court reasoned that allowing the many businesses that operate in both California and single-consent states to record conversations without California consumers’ knowledge or consent would “significantly impair the privacy interests guaranteed by California law” and could place California businesses “at an unfair competitive advantage vis-à-vis their out-of-state counterparts.” Id. The court found California’s interest to be strong because protecting California residents from secret recording was “one of the principal purposes” underlying CIPA, and that subsequent modifications to CIPA demonstrated the Legislature’s continued concern with the same issue. See id. at 124-25. The court further reasoned that the impact on Georgia interests would be minimal because privacy interests protected by

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Georgia law would not be adversely affected, the ruling would affect only calls made to or received from California clients, and the affected companies could still record all such calls so long as they informed consumers at the outset. See id. at 100. Granting deference to companies that had reasonably relied on Georgia law, the Supreme Court declined to impose damages for past conduct in that case, but noted that its ruling should put “out-of-state companies that do business in California . . . on notice that, with regard to future conduct, they are subject to California law with regard to the recording of telephone conversations made to or received from California.” Id. at 130-31.

The same strong California interests apply here as in Kearney. With regard to Nebraska, the relevant statute does appear to give businesses greater latitude to record conversations of their employees than do some other single-consent states. See 5 Leslie T. Thornton & Edward R. McNicholas, Successful Partnering Between Inside and Outside Counsel § 82:55 n.2 (“At least two states . . . require the provision of notice before employers conduct electronic monitoring. Nebraska has taken the contrasting position and enacted an employer friendly law that exempts business from state wiretap statutes and gives employers the right to intercept, disclose and use e-mails in the ordinary course of business.”). Nevertheless, the statute still requires notice to be given to employees when a policy of “service observing or random monitoring” is to be used. Neb. Rev. Stat. § 86-290(2)(a). In fact, Omni, which states that it “set up the Nebraska Call Center to comply with Nebraska law,” DSUF ¶ 3, requires “each Reservation Agent [to] sign[] a document confirming their understanding that Omni may record incoming calls to them, in compliance with Nebraska law,” id. ¶ 4. See also Korner Decl. ¶ 2 (“Reservation Agents are informed that some of their calls are recorded for purposes of employee monitoring, *as Nebraska law requires.*” (emphasis added)).⁶ As in Kearney,

⁶In reply, Omni dismisses these required warnings as “periodic, generic notice” that do not undermine the differences between Nebraska law and the Georgia law considered in Kearney. Because the required notice ensures that each Omni employee participating in a recorded call is aware that her calls with customers are being recorded, the Court does not find the fact that the employees need not consent anew at the outset of each call determinative. In this regard, the Court notes that one of Omni’s primary arguments in opposition to class certification rests upon the proposition that consent can be implied from a general awareness that a call might be recorded, even without actual prior notice at

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

CIPA would only control calls from Californians, and companies would still be able to record calls from California so long as they notified callers at the outset. To the argument that as a practical matter the application of California law would require Omni to change its policies for all incoming calls, the Court finds that Plaintiffs have raised genuine issues of material fact as to the feasibility of determining incoming callers' location and state of residency. See PSDMF ¶ 5. Moreover, Omni's own proffered evidence that being informed of recording at the beginning of a call would not change callers' behavior, see DSUF ¶¶ 9-10, undermines their contention that Nebraska's pro-business interests would be severely hampered by application of CIPA. Overall, the Court finds that the interests of California in the privacy of its consumers would be affected more by the application of Nebraska law than Nebraska's pro-business interests would be affected by the application of California law.

The Court does not find Mazza to be as helpful to Omni as it claims. That case dealt with a putative nationwide class of consumers from 44 states, and the Ninth Circuit noted each state's interest in "having its law applied to its resident claimants" and the importance of federalism concerns in "interstate class actions." 666 F.3d at 592-93 (internal quotation marks omitted) (emphasis added). Here, the putative class is limited to California consumers. Moreover, in California, the "law of the place of the wrong" rule has been subordinated to broader government interest test concerns for decades. See Kearney, 39 Cal. 4th at 108 (explaining that in Reich v. Purcell, 67 Cal. 2d 551, 553-55 (1967), the California Supreme Court "rejected the prior 'law of the place of the wrong' rule as the appropriate choice-of-law analysis, and instead adopted in its place the governmental interest analysis."). Even if the "place of the wrong" were determinative, the California Supreme Court has stated in interpreting CIPA that a telephone conversation between a California resident and an out-of-state business is a "multistate event in which a crucial element—the confidential communication by the California resident—occurred *in California*." Id. at 119 (emphasis in original); see id. ("A person who secretly and intentionally records such a conversation from outside the state effectively acts within California in the same way a person effectively acts within the state by, for example, intentionally shooting a person in California from across the California-Nevada border.")

the outset of the particular call.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

The Court does not dispute the principle that “each state has an interest in setting the appropriate level of liability for companies conducting business within its territory.” Mazza, 666 F.3d at 592 (citing McCann v. Foster Wheeler LLC, 38 Cal. 4th 68, 91 (2010)). But given California’s clearly expressed interest in protecting its residents from secretly recorded phone calls, which the California Supreme Court has found would be seriously impaired by the application of less protective privacy law, and the less clear showing that Nebraska’s interests would be severely impaired by application of California law, the Court finds Kearney’s choice-of-law analysis controlling, and California law applicable to this case.

B. Dormant Commerce Clause

Omni contends that applying § 632.7 as plaintiffs urge would violate the dormant Commerce Clause of the United States Constitution. “Although the Commerce Clause is by its text an affirmative grant of power to Congress to regulate interstate and foreign commerce, the Clause has long been recognized as a self-executing limitation on the power of the States to enact laws imposing substantial burdens on such commerce.” South-Central Timber Dev., Inc. v. Wunnicke, 467 U.S. 82, 87 (1984). “This limitation on state power has come to be known as the dormant Commerce Clause.” Nat’l Ass’n of Optometrists & Opticians v. Harris (Nat’l Ass’n of Optometrists II), 682 F.3d 1144, 1147 (9th Cir. 2012). Modern dormant Commerce Clause jurisprudence “is driven by concern about economic protectionism—that is, regulatory measures designed to benefit in-state economic interests by burdening out-of-state competitors.” Dep’t of Revenue of Ky. v. Davis, 553 U.S. 328, 337-38 (2008). Thus, “not every exercise of local power is invalid merely because it affects in some way the flow of commerce between the states.” Nat’l Ass’n of Optometrists II, 682 F.3d at 1148 (quoting Great Atl. & Pac. Tea Co. v. Cottrell, 424 U.S. 366, 371 (1976)).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Courts evaluating dormant Commerce Clause claims conduct two inquiries.⁷ First, the court “determine[s] whether the statute directly burdens interstate commerce or discriminates against out-of-state interests,” in which case the law is “virtually *per se* invalid and the [c]ourt applies the strictest scrutiny.” LensCrafters, Inc. v. Robinson, 403 F.3d 798, 802 (6th Cir. 2005) (internal quotation marks omitted); see also Nat’l Ass’n of Optometrists & Opticians v. Brown (Nat’l Ass’n of Optometrists I), 567 F.3d 521, 524 (9th Cir. 2009) (“Laws that discriminate against out-of-state entities are subject to strict scrutiny.”). “A statutory scheme can discriminate against out-of-state interests in three different ways: (a) facially, (b) purposefully, or (c) in practical effect.” Nat’l Ass’n of Optometrists I, 567 F.3d at 525 (internal quotation marks omitted). Additionally, a “statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State’s authority.” Healy v. Beer Inst., 491 U.S. 324, 336 (1989); see also Edgar v. MITE Corp., 457 U.S. 624, 640 (1982) (explaining that the Clause “permits only incidental regulation of interstate commerce by the States; direct regulation is prohibited.” (emphasis in original)). But if the law “regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits.” Pike v. Bruce Church, Inc., 397 U.S. 137, 142 (1970). The party challenging the statute “bears the burden of proof in establishing the excessive burden in relation to the local benefits.” Nat’l Ass’n of Optometrists I, 567 F.3d at 528.

1. Per Se Violation of the Dormant Commerce Clause

Omni first contends that application of § 632.7 to these facts would effect direct regulation of extraterritorial commerce, constituting a per se violation of the dormant

⁷A threshold inquiry is whether the Commerce Clause applies at all. The Clause is implicated whenever the regulated activity has a “‘substantial effect’ on interstate commerce such that Congress could regulate the activity.” Conservation Force, Inc. v. Manning, 301 F.3d 985, 993 (9th Cir. 2002) (quoting Camps Newfound/Owatonna, Inc. v. Town of Harrison, 520 U.S. 564, 574 (1997)). This requirement is clearly met here because the conduct at issue involves telephone signals, a channel of interstate commerce that Congress can and does regulate.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Commerce Clause. Omni argues that the fact that § 632.7 “may not facially or even purposefully control out of state interests is not determinative.” Mot. Supp. Summ. J. at 12 (citing Healy, 491 U.S. at 336). In this regard, Omni asserts that because the portability of mobile phone numbers makes it unfeasible to distinguish between Californian and non-Californian calls, compliance with § 632.7 would force Omni to warn all callers, even those from single-consent states, that they could be recorded. Accordingly, Omni argues that this case is like several others in which courts struck down statutes that would have effectively projected state legislation to wholly extraterritorial activity.

Plaintiffs respond that there is no direct extraterritorial regulation here because the telephone calls at issue do not take place wholly outside California. They further argue that § 632.7 does not discriminate in any way because it treats out-of-state and in-state businesses the same: both must obtain consent before recording calls from California customers. Plaintiffs assert that it would be possible for Omni to determine the location of cell phone callers, although Omni responds that each method suggested for doing so impermissibly burdens interstate commerce. Furthermore, plaintiffs argue that the fact that a business may be incentivized to change its practices nationwide to comply with the regulatory policy of one state does not amount to a Commerce Clause violation.

The Court agrees with plaintiffs that this case does not merit strict scrutiny under the dormant Commerce Clause. First, § 632.7 does not discriminate facially, purposefully, or practically against out-of-state commerce. Omni appears to concede that the statute does not discriminate facially or purposefully, and there is case law to that effect. See Zephyr v. Saxon Mortg. Servs., Inc., 873 F. Supp. 2d 1223, 1231 (E.D. Cal. 2012) (“[T]he purpose of California’s Privacy Act does not appear to be to regulate out-of-state commerce or conduct, but to protect California residents from having their conversations recorded by either in-state or out-of-state callers without all parties’ consent.”). Nor does the statute have a discriminatory effect. To make this determination “it is necessary to compare [Omni] with a similarly situated in-state entity.” Nat’l Ass’n of Optometrists I, 567 F.3d at 525. § 632.7 does not place any burdens on out-of-state businesses that do business in California that the law does not place on in-state businesses. See Zephyr, 873 F. Supp. 2d at 1231 (“There does not seem to be any differential treatment of in-state versus out-of-state callers: §§ 632 and 632.7 apply equally to in-state and inter-state calls that are recorded.”); Nader v. Capital One Bank

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

(USA), N.A., cv-12-1265-DSF (RZx), slip op. at 5 n.6 (C.D. Cal. June 11, 2013) (finding that § 632 “operates even-handedly” with regard to in- and out-of-state businesses).

Nor does § 632.7 directly regulate out-of-state commerce in violation of what has been called the “extraterritoriality doctrine.” See Kearney, 39 Cal. 4th at 106-07 (“[T]he occurrences here at issue quite clearly did not take place ‘wholly outside [California’s] borders.’” (brackets in original)). As the Ninth Circuit recently explained, “In the modern era, the Supreme Court has rarely held that statutes violate the extraterritoriality doctrine. The two most prominent cases where a violation did occur both involved similar price-affirmation statutes.” Rocky Mountain Farmers Union v. Corey, 730 F.3d 1070, 1101 (9th Cir. 2013) (discussing Healy v. Beer Inst., Inc., 491 U.S. 324 (1989)). The Ninth Circuit has cautioned that Healy, cited by Omni in support of its extraterritoriality argument, is “not applicable to a statute that does not dictate the price of a product and does not tie the price of its in-state products to out-of-state prices.” Ass’n des Eleveurs de Canards et d’Oies du Quebec v. Harris, 729 F.3d 937, 951 (9th Cir. 2013) (internal quotation marks and brackets omitted); see also Healy, 491 U.S. at 336 (“[S]pecifically, a state may not adopt legislation that has the practical effect of establishing a scale of prices for use in other states.” (internal quotation marks omitted)).⁸ The Ninth Circuit has also distinguished invalid regulations that “directly regulate the actions of parties located in other states” from valid regulations of “relationships in which at least one party is located in California.” Gravquick A/S v. Trimble Navigation Intern. Ltd., 323 F.3d 1219, 1224 (9th Cir. 2003). In Gravquick, the court reasoned that a California law governing business relations among the supply chains of agricultural, utility, and industrial equipment did not violate the dormant Commerce Clause as applied to dealers located outside of California because by contracting with parties located in California, the dealers consented to being governed by California law. See id. Here, as explained above, California law applies to Omni’s telephone conversations with Californians, and out-of-state companies that conduct telephone business with California consumers have been on notice of this at least since Kearney was decided in 2006. This case is therefore different from cases cited by Omni in which a state “projected its legislation” into other states to affect conduct with no California nexus. See, e.g., National Collegiate Athletic

⁸Brown-Forman Distillers Corp. V. New York State Liquor Authority, 476 U.S. 573 (1986), also cited by Omni, similarly involved a price affirmation statute.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

Association v. Miller, 10 F.3d 633, 638 (9th Cir. 1993) (striking down a law “directed at interstate commerce and only interstate commerce” because it regulated “only interstate organizations, *i.e.*, national collegiate athletic associations which have member institutions in 40 or more states”).

Turning to the crux of Omni’s argument, Omni’s claims that application of § 632.7 forces Omni as a practical matter to change its handling of callers from every state are insufficient to show a constitutional violation at this stage of the litigation. The calls at issue involved telephonic connections between California and Nebraska, and it was Californians who allegedly had their conversations recorded without forewarning. See Zephyr, 873 F. Supp. 2d at 1230 (“California §§ 632 and 632.7 do not regulate conduct that occurs in entirely another state as Saxon’s calls are made to California residents’ telephones and the conversations are made with California residents.”). Although the portability of mobile phone numbers may make it difficult to know with certainty whether a caller is indeed calling from or residing in California, viewing the evidence in the light most favorable to plaintiffs as the Court is required to on a motion for summary judgment, there is at least a triable issue of fact as to whether it would be “futile” for Omni to differentiate among Californian and non-Californian callers. See PSDMF ¶ 5.

Moreover, legislation that may cause businesses to decide to conform nationwide conduct to meet the requirements of a given state does not necessarily constitute direct regulation of out-of-state commerce. “Courts have held that when a defendant chooses to manufacture one product for a nationwide market, rather than target its products to comply with state laws, defendant’s choice does not implicate the commerce clause.” Nat’l Fed’n of the Blind v. Target Corp., 452 F. Supp. 2d 946, 961 (N.D. Cal. 2006); see id. (“[E]ven if [defendant] chooses to change its entire website in order to comply with California law, this does not mean that California is regulating out-of-state conduct.”). The Ninth Circuit has recently held that “regulation with reference to local harms” does not constitute extraterritorial regulation under the Commerce Clause merely because that regulation creates incentives for businesses to alter out-of-state activity. Rocky Mountain Farmers Union, 730 F.3d at 1101-06 (holding that California fuel standards taking into account “lifecycle” emissions did not “control conduct wholly outside the state” despite arguments that the standards forced plaintiffs to conform out-of-state conduct to California law). Similarly, § 632.7 regulates only calls with a nexus to California and has the purpose of preventing privacy harms to Californians, even if it might create

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

incentives for Omni to alter its behavior nationwide. Cf. Kearney, 39 Cal. 4th at 10-054 (“[A] company that conducts business in numerous states ordinarily is required to make itself aware of and comply with the law of a state in which it chooses to do business. . . . [A] state generally does not exceed its constitutional authority when it applies a law in such a setting, even if the law may implicate some action . . . that occurs outside the state.”).⁹ That Omni may find it more convenient to warn all callers that their calls may be recorded, rather than attempt to differentiate between callers from single-consent and dual-consent states, does not create a constitutional violation. Cf. Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 1265 (stating that a company’s “business decision” to comply with the statute all the time to avoid a determination of whether the company is corresponding with a California resident in each instance “does not establish that [the statute] controls conduct occurring wholly outside California”). To the extent that § 632.7 affects out-of-state commerce, such effects are “incidental” and do not constitute direct regulation meriting strict scrutiny under the dormant Commerce Clause.

2. Undue Burden on Interstate Commerce

Omni argues in the alternative the requested application of § 632.7 would impose incidental burdens on interstate commerce that clearly outweigh the local benefits secured. Omni contends that compliance with § 632.7 “provides no real benefit whatsoever” for several reasons. First, Omni avers that many California callers assume their calls to hotels are recorded even absent a warning. Second, Omni disputes that Omni’s recording of telephone calls without a warning affected plaintiffs in any way. Third, Omni argues that § 632.7 does not protect Californians’ confidential communications. Fourth, Omni contends that the statute does not benefit consumers whose calls were recorded for service observing purposes as opposed to intercepted by a

⁹Although the Kearney court made this determination in the context of choice of law and due process arguments, the Court finds the facts and legal issues similar enough to make the court’s reasoning relevant and persuasive. See Donald H. Regan, Siamese Essays: (I) CTS Corp. V. Dynamics Corp. of America and Dormant Commerce Clause Doctrine; (II) Extraterritorial State Legislation, 85 Mich. L. Rev. 1865, 1884-85 (1987) (noting that courts deciding conflict-of-laws cases have addressed extraterritoriality issues similar to those treated under the dormant Commerce Clause).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

third party. Conversely, Omni argues, the “burdens on interstate commerce are extraordinary.” Omni cites the potential damages in this case as well as the fact that this lawsuit has already “coerced Omni into warning every caller that he or she may be recorded.”

Plaintiffs deny that Omni has shown any burden imposed on it by application of § 632.7. They point out that, following this lawsuit’s filing, Omni added an automated notification of potential recording for each caller, and assert that adding the recording cost Omni only about an hour’s worth of employee labor. PSDMF ¶ 13. Plaintiffs also deny that Omni has presented evidence that having to inform callers of potential recording has adversely impacted Omni. On the benefits side of the equation, plaintiffs argue that 632.7 protects strong privacy interests ignored by Omni.

Despite Omni’s argument that § 632.7’s application to Omni’s conduct provides “no real benefit whatsoever,” this Court finds persuasive the California Supreme Court’s reasoning that refusing to apply the law to similar conduct would “significantly impair the privacy policy guaranteed by California law.” Kearney, 39 Cal. 4th at 100. Against these real local interests, the Court does not find that Omni has shown clearly excessive burdens on interstate commerce.¹⁰ As stated above, plaintiffs have at least raised a genuine issue of material fact as to whether Omni could feasibly “comply with California

¹⁰The Court does not find Omni’s citation of several cases involving internet content regulation persuasive as to either the extraterritoriality of or the interstate burden imposed by § 632.7, chiefly because the nature of the internet and the conduct regulated in those cases directly extended the regulation to persons with no connection to the regulating state. See Mot. Summ. J. at 15, 17-18. The Court also finds inapposite Consolidated Cigar Corp. v. Reilley, 218 F.3d 30 (1st Cir. 2000), rev’d in part on other grounds sub nom. Lorillard Tobacco Corp. v. Reilly, 533 U.S. 525 (2001). In that case, the statute imposed liability for advertising without required health warnings in national magazines distributed in Massachusetts, as well as for advertising on the internet that could be “viewed from a terminal” in the state. Id. at 56. Therefore, unlike here, the statute directly regulated and placed burdens on conduct outside of the state. This is very different from Omni’s argument that it is easier for Omni to play the same five-second recording for every caller than to determine the origin of each call.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

law without altering its conduct with regard to non-California clients.” Kearney, 39 Cal. 4th at 107; Mem. Supp. Mot. Summ. J. at 17; see PSDMF ¶ 5. Even if that were not the case, Omni has not met its burden at this stage of the litigation of proving that the burden of complying with § 632.7 is “clearly excessive in relation to the putative local benefits.” Pike, 397 U.S. at 142.¹¹

C. Excessive Damages

Omni next argues that the statutory damages sought by plaintiffs are unconstitutional under the Excessive Fines Clause, U.S. Const. amend. VIII, and due process principles.

The Excessive Fines Clause is inapplicable where, as here, civil damages are sought in a lawsuit between private parties. United States v. Bajakajian, cited by Omni in support of its argument, explains that “fine” as used in the Eighth Amendment means “a payment to a sovereign as punishment for some offense.” 524 U.S. 321, 327 (1998) (emphasis added) (quoting Browning-Ferris Indus. Of Vt., Inc. v. Kelco Disposal, 492 U.S. 257, 265 (1989)). An earlier Supreme Court case succinctly states the flaw in Omni’s argument: the Eighth Amendment “does not constrain an award of money damages in a civil suit when the government neither has prosecuted the action nor has any right to receive a share of the damages awarded.” Browning-Ferris, 492 U.S. at 264. The Browning-Ferris Court explained that its “concerns in applying the Eighth Amendment have been with criminal process and with direct actions initiated by government to inflict punishment.” Id. at 260. See also Zomba Enter., Inc. v. Panorama Records, Inc., 491 F.3d 574, 586 (6th Cir. 2007) (citing Bajakajian and Browning-Ferris in rejecting an argument that the Eighth Amendment applied to enhanced statutory damages under the Copyright Act).

At this stage of the litigation, Omni’s argument that the statutory damages violate due process must also be rejected. In fact, one of the two opinions Omni cites in support

¹¹The Court agrees with plaintiffs that the statutory damages sought in this case are a potential penalty for failing to comply with California law, not a burden on interstate commerce resulting from compliance.

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

of its due process contentions declined at a similar juncture to consider an argument that statutory damages were excessive. See In re Napster, Inc. Copyright Litig., No. C MDL-00-1369 MHP, 2005 WL 1287611, at *11 (N.D. Cal. June 1, 2005). On a motion for class certification, that court found that “at this stage of the proceedings, there is simply nothing in the record that would permit the court to apply” the reasonableness guideposts urged by Omni “in an informed manner,” and that any inquiry would be “speculative, based on a potential statutory maximum award rather than an actual jury verdict.” Id.; see also Centerline Equip. Corp. v. Banner Personal Serv., Inc., 545 F. Supp. 2d 768, 778 (N.D. Ill. 2008) (“It is premature at this [class certification] stage to consider whether any hypothetical [statutory damages] award might be constitutionally excessive.”); DirecTV v. Spillman, No. Civ.A.SA-04-82-XR, 2004 WL 1875045, at *4 (W.D. Tex. Aug. 23, 2004) (declining to consider due process objections to potential statutory damages on a motion to dismiss because such an argument was “premature”). Additionally, in tension with Omni’s use of the case, In re Napster questioned the notion that statutory damages should be “singled out for heightened scrutiny” under the Due Process Clause. 2005 WL 1287611, at *11; see id. (“[T]he conclusion that class action treatment might somehow influence the proportionality of a statutory damages award is logically flawed.”).¹²

¹²The Court is not persuaded to consider Omni’s arguments at this juncture by Cohorst v. BRE Props., Inc., No. 3:10-cv-2666-JM-BGS, 2011 WL 7061923 (S.D. Cal. Nov. 14, 2011). First, that report of a special master reviewed an actual settlement as opposed to a hypothetical maximum damages award. Second, that report applied Excessive Fines Clause jurisprudence to a statutory damages award in a case between private parties, see id. at *14, despite the U.S. Supreme Court’s clear rule that the clause “limit[s] only those fines directly imposed by, and payable to, the government,” Browning-Ferris, 492 U.S. at 268. In doing so, the report relied on a California Supreme Court case that involved civil fines sought by the California Attorney General, a situation that *would* implicate the Eighth Amendment’s concern with proceedings brought by the government. See generally People ex rel. Lockyer v. R.J. Reynolds Tobacco Co., 37 Cal. 4th 707 (2005).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

D. § 632.7's Applicability to Call Participants

Next, Omni argues that § 632.7 does not apply to call participants based on differences between the language in that provision and § 632. Specifically, § 632 holds liable anyone who “eavesdrops upon or records” a telephone communication, and § 632.7 imposes liability on anyone who “intercepts or receives and records” a cellular telephone call. Omni first cites general principles of statutory interpretation to argue (1) that “intercepts or receives” would be extraneous if § 632.7 applied to parties, and (2) that the use of “receives” in §§ 632.5 and 632.6 to apply to third parties shows that “receives” should be read to only apply to third parties in § 632.7. Omni then turns to legislative history it argues “demonstrates that the drafters sought only to fill a perceived gap in the statutory scheme by merely extending sections 632.5 and 632.6, which required malice, to non-malicious third-party recordings.” Mem. Supp. Summ. J. at 21. Omni also claims that the legislative history and potential “absurd and unfair results” justifies “qualify[ing] the plain meaning” of 632.7. *Id.* at 24 (citing Ctr. For Nat’l Policy Review on Race & Urban Issues v. Weinberger, 502 F.2d 370, 374 (D.C. Cir. 1974)). In response, plaintiffs stress that 632.7 uses the word “receive” in addition to the word “intercept,” implying that the words have different meanings. They also cite recent cases rejecting the construction Omni urges.

The Court agrees with the decisions cited by plaintiff, and finds that § 632.7 prevents a party to a cellular telephone conversation from recording it without the consent of all parties to the conversation. See Montantes v. Inventure Foods, No. cv-14-1128-MWF (RZx), 2014 WL 3305578, at *2-4 (C.D. Cal. July 2, 2014) (“The text of § 632.7 unambiguously includes a person who ‘receives a protected ‘communication,’ whether or not the communication is received while in transit or at its destination.”); Kuschner v. Nationwide Credit, Inc., 256 F.R.D. 684, 688 (E.D. Cal. 2009) (construing § 632.7 to apply to a claim that one party to a telephone conversation had recorded it without the other party’s consent). As this Court has previously stated, this interpretation flows from the clear and unambiguous language of the statute. Brown v. Defender Sec. Co., No. cv-12-7319-CAS (PJWx), 2012 WL 5308964 (C.D. Cal. Oct. 22, 2012). Initially, as a matter of common usage, the participants in a conversation “receive” communications from each other. This alone suggests that § 632.7 should not be limited to situations in which unknown third parties record a conversation. Additional support for

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

the Court's interpretation lies in the fact that the statute uses the terms “receives” and “intercepts” disjunctively, which suggests that these terms are meant to apply to distinct kinds of conduct. Since “intercepts” is most naturally interpreted to refer to conduct whereby an unknown party secretly accesses a conversations, “receives” is naturally read to refer to something other than access to a conversation by an unknown interloper.¹³

E. “Injury” Under § 632.7

Finally, Omni contends that plaintiffs cannot sustain an action under § 632.7 because they cannot demonstrate that they have suffered an injury. Plaintiffs respond that Omni’s alleged violation of CIPA is “itself a legally cognizable injury giving rise to the right to recover statutory damages,” and that they “are not required to show any financial or other injury.” PSDMF ¶ 10. Omni argues that plaintiffs’ argument relies on a conflation of the terms “injury” and “damages.”

The Court concurs with cases cited by plaintiffs finding that, in light of the California legislature’s decision to create statutory damages for each violation of CIPA, no separate showing of injury aside from a violation of the privacy rights protected by CIPA is required. See, e.g., *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS172784, at *65-67 (N.D. Cal. Sep. 26, 2013) (rejecting an argument that § 632.7 requires independent injury aside from an invasion of statutory CIPA rights); *Lieberman v. KCOP Television, Inc.*, 110 Cal. App. 4th 156, 167 (2003) (“[A]n actionable violation of section 632 occurs the moment the surreptitious recording is made.”); *Friddle v. Epstein*, 16 Cal. App. 4th 1649, 1661 (1993) (holding that the right to recover statutory damages “accrue[s] at the moment the Privacy Act was violated”). This finding is bolstered by the fact that § 637.2 provides for damages of “the greater of”

¹³Because the Court finds the statutory language unambiguous, it does not consider legislative history. *Viceroy Gold Corp. v. Aubry*, 75 F.3d 482, 490 (9th Cir.1996); *Delaney v. Superior Court*, 50 Cal. 3d 785, 798 (Cal.1990). The Court notes, however, that at least one district court has investigated the legislative history and found, contrary to Omni’s assertions, that “[i]nterpreting § 632.7 to only apply to third parties would defeat the Legislature's intent.” *Simpson v. Best Western Int’l, Inc.*, No. 3:12-cv-04672-JCS, 2012 WL 5499928, at *9 (N.D. Cal. Nov. 13, 2012).

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

“O”

CIVIL MINUTES - GENERAL

Case No.	2:13-CV-2468-CAS(MANx)	Date	September 8, 2014
Title	STEVEN ADES, ET AL. v. OMNI HOTELS MANAGEMENT CORP., ET AL.		

\$5000 or “[t]hree times the amount of actual damages, *if any*, sustained by the plaintiff,” and states that it is “not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.” Cal. Penal Code § 637.2(a), (c). The Court is not convinced that the Legislature intended to require some showing of injury in addition to a violation of privacy rights under CIPA, but not necessarily including actual damages. Put simply, “[t]he harm consists of the unauthorized recording.” California Practice Guide: Civil Procedure Before Trial Claims & Defenses § 4:1690.¹⁴

V. CONCLUSION

For the foregoing reasons, Omni’s motion for summary judgment is DENIED.

IT IS SO ORDERED.

Initials of Preparer

00 : 16

CMJ

¹⁴Omni relies heavily on a Superior Court’s order in Hopkins v. Healthmarkets, No. BC404133, 2011 WL 7463408 (L.A. Sup. Ct. Nov. 30, 2011). That order did not discuss the cases cited above, or any other case law, with regard to the injury requirement of § 637.2. The Court acknowledges the Hopkins case’s support for Omni’s position but respectfully disagrees with its conclusion.

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

HYO JUNG, et al.,

Plaintiffs,

- against -

CHORUS MUSIC STUDIO, INC., et al.,

Defendants.

⌋
:
:
:
:
:
:
:
:
:
⌋

OPINION AND ORDER

13-CV-1494 (CM) (RLE)

RONALD L. ELLIS, U.S.M.J.:

I. INTRODUCTION

Plaintiffs Hyo Jung, Kee Soo Hong, JeongMin Song, HaeYong Lee, Dal Young Cho, Kyungmo Yan, and SangYoon Shin (“Plaintiffs”) commenced this action on March 5, 2013, alleging wage and hour violations under the Fair Labor Standards Act, 29 U.S.C. §§ 201, et seq. (“FLSA”) and New York Labor Law (“NYLL”) and its accompanying regulations. (Compl. ¶¶ 27-54.) Plaintiffs were waiters and busboys at Defendants’ karaoke lounge, Chorus Karaoke. This action was referred to the undersigned on October 4, 2013, for a specific discovery dispute, (Docket No. 11), which was resolved at a telephone conference with the Parties on October 21, 2013. On October 29, 2013, the case was referred for Defendants’ motion to amend their Answer to include counterclaims under the Computer Fraud and Abuse Act, 28 U.S.C. § 1030(a) et seq. (“CFAA”) and under common law theories of conversion, misappropriation of trade secrets, and unjust enrichment. (Docket No. 15.) For the reasons which follow, Defendants’ motion is **DENIED**.

II. BACKGROUND

Plaintiffs were employed by Defendants in various years spanning 2008 to 2012. Defendants allege that all of the Plaintiffs quit their employment on February 10, 2013, (Def. Mem. Of Law. In Supp. Of Mot. To Amend (“Def Mem.”) at 4), and Plaintiffs do not dispute that fact. (Pl. Mem. Of Law In Opp. To Mot. To Amend (“Pl. Mem.”) at 23.) On April 16, District Judge Colleen McMahon issued a scheduling order which set July 1 as the deadline for amending the pleadings. Plaintiff served discovery requests on April 22 and Defendants served discovery requests on May 18. Plaintiffs produced documents in response to Defendants’ discovery requests on June 28, including the “customer list” at issue in Defendants’ proposed counterclaims.

On July 9, and August 1, 2013, Plaintiffs took the Rule 30(b)(6) deposition of the corporate Defendants. On July 24, Defendants served a notice of deposition on Plaintiff Jung for August 22, and subsequently cancelled that date, and Jung was deposed on September 24. Plaintiff Hong was deposed on October 1. At his deposition, Hong testified that: “[T]here was an occasion when the shop had to change the computer and at that time, the manager instructed me to back up the information that had been stored in the previous computer in a file. So I forwarded the content to my own e-mail address when the computer was removed and I stored the information that had been installed in my e-mail account and that was it. I never opened them.” (Pl. Decl. In Opp. To Mot. To Amend (“Pl. Decl.”) Ex. 3 at 23:13-23.) Hong later testified that, although he did not know what was contained in the file, he sent it to Plaintiffs’ counsel “so that they can see if the files could be of some use and help the case.” (*Id.* at 25:21-25.)

The deposition of Hong began on October 3, 2013, but was interrupted by a dispute over the deposition. On October 21, the Parties appeared before the Court for a telephone conference to address discovery disputes. At the conference, the Court ordered Plaintiffs' counsel to forward by email to Defendants' counsel any electronic files in her possession that were sent to her by Hong. On October 24, Plaintiffs' counsel forwarded three emails from Hong to Defendants' counsel. (Def. Decl. In Supp. Of Mot. To Amend, Ex. D.) Defendants acknowledged receipt of the emails, but disputed the completeness of the submission. (Docket No. 14.)

Defendants allege that, in April 2013, Plaintiffs initiated their own business venture, Club 88 NY. Defendants seek to rely on the deposition of Jung for this assertion. The pages Defendants provided from Jung's deposition indicate that Jung coordinated with a person named "Michael Yoo" to rent a space for parties with certain unnamed individuals, that the space was called "Club 88" on party days, and that Jung was referred to Michael Yoo by a man named "Haeyong," whose American name was "Michael." (Def. Decl. Ex. F.) Defendants assert that Plaintiffs used Defendants' customer list and other proprietary information taken by Hong from Defendants' computer to promote their new venture, citing Exhibit G, which appears to be a printout from the website of Club 88 NY. Plaintiffs dispute both of these allegations. With respect to Club 88 NY, they do not dispute that the named Plaintiffs worked together at some point in time after leaving Defendants' employ, but dispute that all of the named Plaintiffs worked together for Club 88 NY. (Pl. Mem. at 23.) With respect to the customer list, Defendants allege that since Plaintiffs left their employment, their business has suffered a "significant downturn." (Def. Lee Decl. ¶ 9.) Defendants stated at the October 21 Telephone

Conference for the first time that they intended to move to amend their Answer to add counterclaims. Defendants filed the instant motion on November 4, 2013.

III. DISCUSSION

A. The Motion to Amend Should Be Denied Under Rule 16(b)

Generally, leave of court to amend pleadings should be freely given when justice so requires. Fed. R. Civ. P. 15(a); *Rachman Bag Co. v. Liberty Mut. Ins. Co.*, 46 F.3d 230 (2d Cir. 1995), *aff'd*, 101 F.3d 1393 (2d Cir. 1996). However, a party moving to amend the pleadings made after the deadline to do so in the court's scheduling order must first satisfy the good cause requirement of Federal Rule of Civil Procedure 16(b). Fed. R. Civ. P. 16(b). *See Parker v. Columbia Pictures Industries*, 204 F.3d 326, 339-40 (2d Cir. 2000). "A finding of 'good cause' depends on the diligence of the moving party." *Id.* at 340. Although diligence is "the primary consideration," the court may consider other relevant factors, including whether amendment of the pleadings will prejudice the opposing party. *Kassner v. 2nd Avenue Delicatessen, Inc.*, 496 F.3d 229, 244 (2d Cir. 2007); *Grant v. Citibank*, 10-CV-2955 (KNF), 2010 WL 5187754 (S.D.N.Y. Dec. 6, 2010). If a proposed amendment is based on "information that the party knew or should have known prior to the deadline, leave to amend is properly denied." *Soroof Trading Dev. Co., Ltd. V. GE Microgen, Inc.*, 283 F.R.D. 142, 147 (S.D.N.Y. 2012). *See Fuller v. Interview, Inc.*, 07-CV-5728 (RJS) (DF).

Defendants did not act with diligence in pursuing their motion to amend. Defendants filed the motion to amend on November 4, 2013, over four months after the deadline for amendment of pleadings, July 1, 2013. Defendants assert that they were unaware of the facts underlying their counterclaims until Hong's deposition on October 1, 2013. (Def. Lec. Decl. ¶ 4.) However, Plaintiffs assert, and Defendants do not dispute, that on May 18, 2013, Defendants

sent Plaintiffs their document requests, including a request that Plaintiffs “[p]roduce all documents in the form when they were taken, including invoices, receipts, customer information, or other employee’s information which are the property of the Employer that each Plaintiff without permission, may have removed from Chorus’s place of business at any time during their employment with Chorus.” (Pl. Schulman Decl. Ex. 2 at 5.) On June 28, Plaintiffs responded to Defendants’ document requests, and, among other documents, produced the customer list now at issue. (Pl. Schulman Decl. ¶ 8.) The production of the list at issue before the deadline for amendments to the pleadings, if not the original request for the list, demonstrates that Defendants knew or should have known the facts underlying their counterclaims prior to the deadline. *Soroof Trading Dev. Co., Ltd.*, 283 F.R.D. at 147.

Defendants assert that Plaintiffs merely produced print-outs or hard copy documents in response to their May 18, 2013 discovery request, and that they were not on notice that documents had been taken from Defendant Chorus’s business computer until they received documents in electronic form from Plaintiffs’ counsel pursuant to the Court’s order. This argument is without merit. Whether or not Defendants knew of the facts supporting the counterclaims is not the standard. The record shows that even if Defendants did not know the facts underlying their proposed claims before July 1, 2013, they should have known.

Defendants also failed to act with diligence by not requesting an extension of the deadline as soon as they received the customer list from Plaintiffs. Even crediting Defendants’ claim that they were unaware of the alleged unauthorized taking of electronic information before October 1, 2013, Defendants did not act with diligence when they failed to notify the Court about their intended motion to amend before the October 21, 2013 Telephone Conference. Defendants correctly assert that they notified the Court of Hong’s alleged unauthorized taking of the files on

October 4, 2013, but failed to notify the Court of their intent to amend the pleadings. Defendants also delayed in serving their discovery requests for over a month after the scheduling order was issued, (Pl. Schulman Decl. ¶¶ 3, 6), and despite appearing to suspect that some of their former employees could have taken documents from Chorus without permission, failed to serve any requests seeking the identity of the person or persons in possession of such documents. Defendants also delayed the start of depositions by cancelling a deposition scheduled for August 22, 2013. (*Id.* ¶ 12.) Defendants' cumulative actions show a general lack of urgency.

Granting Defendants' motion to amend would also prejudice Plaintiffs. In assessing prejudice, courts consider whether the amendment of the pleadings would "(i) require the opponent to expend significant additional resources to conduct discovery and prepare for trial; (ii) significantly delay the resolution of the dispute; or (iii) prevent the plaintiff from bringing a timely action in another jurisdiction." *Block v. First Blood Associates*, 988 F.2d 344, 350 (2d Cir. 1993). In this case, amendment of the pleadings would require Plaintiffs to "expend significant additional resources to conduct discovery and prepare for trial" and significantly delay resolution of the case. *Id.* Pursuant to Judge McMahon's April 16, 2013 scheduling order, discovery was ordered closed on November 1, 2013,¹ (Pl. Schulman Decl. Ex. 1), and document discovery and two of seven of depositions have already been completed. (Def. Mem. at 21.) Defendants' proposed counterclaims for conversion, misappropriation of trade secrets, and unjust enrichment, and violations of the CRFAA are factually unrelated to Plaintiffs' wage and hour claims, and would therefore require a new round of discovery. *See Gallagher's NYC Steakhouse Franchising, Inc. v. N.Y. Steakhouse of Tampa, Inc.*, 11-CV-1456 (THK), 2011 WL 6034481, at

¹ Judge McMahon has authorized the undersigned to extend discovery if the instant motion is granted. (Docket No. 18.)

*8 (S.D.N.Y. Dec. 5, 2011) (“Granting Defendants’ motion would require reopening discovery on a different set of facts than those in the present pleadings.”).

Defendants assert that Plaintiffs are not prejudiced because the counterclaims are “based on Plaintiffs’ conduct and transactions that occurred during the Plaintiffs’ employment with the employer Chorus they were at all times on notice of the conduct at issue in Defendants’ counterclaims.” (Def. Mem. Of Law in Supp. Of Mot. To Amend (“Def. Mem.”) at 21.)

Defendants also argue that Plaintiffs were on notice because “Plaintiff Hong freely discussed and admitted to taking Chorus’ proprietary electronic information and transferring it to his personal email.” (*Id.*) However, Defendants do not assert that Plaintiff Hong admitted to taking and transferring the electronic information without authorization. To the contrary, Plaintiffs contest Defendants’ assertion that Plaintiff Hong had no authorization. Defendants’ allegations cannot be presumed to be true for the purposes of assessing prejudice to Plaintiffs.

Defendants further argue that Plaintiffs would not be prejudiced because Plaintiffs have delayed discovery by improperly halting a deposition on October 3, 2013, by failing to produce the documents requested on May 18, 2013 in electronic form, and through Plaintiffs’ counsel delaying admitting that she was in possession of Chorus’s electronic proprietary information until October 21, 2013 and being unavailable during September 2013 for depositions.

Defendants further assert that Plaintiffs were complicit in the delay of discovery because they were unavailable for most of September 2013, (Def. Ghim Decl. Ex. J), and they did not oppose Defendants’ request to extend discovery to November 1, 2013. (*Id.* Ex. K.) Defendants cite *Grant v. Citibank* for the proposition that non-movants cannot show that a movant’s delay was significant if they participated in causing it. 2010 WL 5187754, at *24-25. Defendants’ arguments are without merit. Defendants have not shown that Plaintiffs have unnecessarily

delayed discovery to the point that they cannot claim to be prejudiced by Defendants proposed counterclaims. Additionally, *Grant v. Citibank* is distinguishable because the non-movants participation in the delay was significant in that the non-movants failed to respond to the movant's request for consent to amend his complaint, engaged in settlement in negotiations concerning the new claims, and ultimately ended the settlement negotiations by filing a motion for summary judgment. *Id.*

Finally, Defendants assert that Plaintiffs would not be prejudiced by further discovery because discovery has not been completed, and depositions of five of the seven Plaintiffs are still pending. Defendants are correct that this case is distinct from *Gallagher's NYC Steakhouse Franchising, Inc.* in that Judge McMahon has authorized the undersigned to extend discovery if the instant motion is granted. (Docket No. 18.) However, Plaintiffs would still be prejudiced by the addition of an extra round of discovery on factually unrelated counterclaims.

Defendants have failed to meet the "good cause" requirements of Rule 16(b). The motion to amend is **DENIED**.

B. The Motion to Amend Should Be Denied Under Rule 15(a)

Even were the Court to find that Defendants had met the good cause standard under Rule 16(b), the motion to amend would fail under Rule 15(a). Although leave to amend the pleadings should be "freely given" under Rule 15(a), Fed. R. Civ. P. 15(a), "[r]easons for a proper denial of leave to amend include undue delay, bad faith, futility of the amendment, and perhaps most important, the resulting prejudice to the opposing party." *State Teachers Retirement Board v. Fluor Corp.*, 654 F.2d 843, 856 (2d Cir. 1981); *Duhos v. Floating and Abandoned Vessel, Known as New York*, 162 F.3d 63, 69 (2d Cir. 1998). Mere delay, absent a showing of bad faith or undue prejudice by the nonmovant, is not sufficient to deny the right to amend a pleading.

Fluor, 654 F.2d at 856. Where discovery has been closed, subsequent amendment of the pleadings may be found to prejudice the opposing party. *Berman v. Parco*, 986 F. Supp. 195 (S.D.N.Y. 1996).

In determining what constitutes prejudice, the court considers whether the assertion of the new claim would (1) require the opponent to expend significant additional resources to conduct discovery and prepare for trial; (2) significantly delay the resolution of the dispute; or (3) prevent the plaintiff from bringing a timely action in another jurisdiction. *Block v. First Blood Associates*, 988 F.2d 344, 350 (2d Cir. 1993); *Duncan v. College of New Rochelle*, 174 F.R.D. 48, 49 (S.D.N.Y. 1997). Additionally, leave to amend may be denied where the moving party knows or should have known the facts upon which the amendment is based, but did not originally plead them. *Priestly v. American Airlines, Inc.*, 1991 WL 64459 (S.D.N.Y. 1991).

Where there is undue delay in filing a motion under Rule 15(a), the movant must provide a satisfactory answer for the delay. *Lightfoot v. Union Carbide Corp.*, 1997 WL 752357, *2 (S.D.N.Y. Dec. 2, 1997) (citing *Cresswell v. Sullivan & Cromwell*, 922 F.2d. 60, 72 (2d Cir. 1990)). As discussed in the preceding section, Defendants acted with undue delay in pursuing the motion to amend. However, even if the Court were to find that Defendants did not act with undue delay, Defendants' proposed conversion, misappropriation of trade secrets, and unjust enrichment counterclaims and Defendants' proposed CFAA counterclaim against Plaintiffs Hyo Jung, JeongMin Song, HaeYong Lee, Dal Young Cho, Kyungmo Yan, and SangYoon Shin are futile, and therefore the motion to amend should be **DENIED** with respect to those claims. Defendants' CFAA counterclaim against Plaintiff Hong is not futile, and therefore Defendants' motion would be viable with respect to that counterclaim.

1. Defendants' proposed counterclaim under the CFAA is futile against all the named Plaintiffs except Hong.

Under the CFAA, "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section." 18 U.S.C. §§ 1030(a)(2), (a)(7). Defendants assert that Hong accessed Defendant Chorus Music Studio's business computer without authorization. The CFAA permits a civil action where there has been damage or loss and "conduct involv[ing] 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g).

Defendants assert that Hong's actions "caused damage or loss in excess of \$5,000 in one year to one or more persons." 18 U.S.C. §§ 1030(c)(4)(A)(i)(I)-(V). The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(c)(11).

Plaintiffs assert that Defendants have only alleged that Hong misused the information in Chorus's business computer by transferring it to his own email account, and have not alleged that he did not have authorization to access the computer. Plaintiffs argue that courts in this district have interpreted the CFAA as prohibiting only unauthorized access to information, and not misuse of information. *See JBC Holdings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 523 (S.D.N.Y. 2013) ("When an employee who has been granted access to an employer's computer misuses that access, either by violating the terms of use or by breaching a duty of loyalty to the employer, the employee does not 'exceed authorized access' or act 'without authorization.'"); *Orbit One Commc'ns, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) ("The

CFAA . . . does not prohibit misuse or misappropriation [of computer information].”) Although the Second Circuit has not ruled on the issue, Plaintiffs assert that the Second Circuit’s decision in *Nexans Wires S.A. v. Sark-USA, Inc.* supports a narrow interpretation of the CFAA. 166 F. App’x 559, 562 (2d Cir. 2006) (denying remedy under CFAA for revenue lost due to misappropriation of information).

Plaintiffs’ arguments are unpersuasive. In their proposed First Amended Answer, Defendants assert that “Plaintiff Hong intentionally stole electronic proprietary information when he transferred all electronic files from Chorus’ business computer to his personal e-mail without authorization.” (Def. Decl. Ex. A ¶ 103.) Defendants also assert that Plaintiff Hong was “not needed or asked, at any relevant time to . . . access the business computer.” (*Id.* at ¶ 96.) Defendants have alleged misuse or misappropriation of electronic information but not unauthorized access. The Second Circuit has not ruled on what elements constitute violations of the CFAA, and not all courts in this district have adopted Plaintiff’s narrower interpretation of the CFAA. In *Calyon v. Mizuho Secs. USA, Inc.*, for example, the court reasoned that “the plain language of the statute seems to contemplate that . . . ‘without access’ and ‘exceeds authorized access’ would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer” and found that employees who transferred information from their employer’s computer to their personal email accounts before starting work at another company violated the CFAA. No. 07-CV-2241 (RO), 2007 WL 2618658, at *1 (S.D.N.Y. July 24, 2007). Because Defendants’ proposed counterclaims need only be plausible to be considered not futile, *N.H. Ins. Co. v. Total Tool Supply, Inc.*, 621 F. Supp. 2d 121, 124 (S.D.N.Y. 2009), the Court finds that Defendants’ proposed claims would be allowable against Hong.

Plaintiffs also argue that Defendants have not plausibly alleged that Hong's actions "caused damage or loss in excess of \$5,000 in one year to one or more persons." 18 U.S.C. §§ 1030(c)(4)(A)(i)(I)-(V). In their proposed First Amended Answer, Defendants assert that "[a] damage assessment is still ongoing and the scope of the damage has still not been determined to date. However, Defendants have spent at least \$5,000 to respond to the theft and assess the damage within the meaning of the CFAA." (Def. Decl. Ex. A ¶ 81.) Plaintiffs claim that Defendants' allegations regarding damages are "formulaic recitation[s] of the elements" of a claim and insufficient to meet the plausibility standard under *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). However, for the purposes of deciding a motion to dismiss pursuant to Rule 12(b)(6), the issue is "not whether a [party] will ultimately prevail but whether the claimant is entitled to offer evidence to support the claims." *York v. Ass'n of Bar of City of New York*, 286 F.3d 122, 125 (2d Cir. 2002). Defendants' proposed counterclaims allege sufficient facts to support a claim under the CFAA.

Plaintiffs further assert that it is not plausible that Defendants could have incurred a loss of \$5,000 or more. To support this proposition, Plaintiffs cite a single case where damages based on cost of assessment was less than \$5,000. *See, e.g., Int'l Chauffeured Serv., Inc. v. Fast Operating Corp.*, 11-CV-2662 (NRB), 2012 WL 1279825, at *4 (S.D.N.Y. Apr. 16, 2012). Plaintiffs have not shown that Defendants' claim regarding damages is implausible. Accordingly, Defendants' CFAA claim is not clearly futile against Hong.

Defendants CFAA claim against the other named Plaintiffs, however, is futile. Defendants assert that the other named Plaintiffs conspired with Hong to use the proprietary information Hong took from Defendants' business computer to promote their new business venture. (Def. Decl. Ex. A ¶ 85.) To support their conspiracy allegation, Defendants make a

number of conclusory allegations, including: 1) “Plaintiff Hong conspired with other named Plaintiffs in the main action to take Chorus’ proprietary information for use in a lawsuit against Defendants while they were still employed at Chorus;” (*Id.* ¶ 85); 2) “Plaintiffs aided and abetted Plaintiff Hong in the theft of Chorus’ electronic proprietary information” (*Id.* ¶ 104); 3) “Plaintiffs sold the subject customer lists to third parties and unjustly enriched themselves” (*Id.* ¶ 105); and 4) “Plaintiffs contacted or solicited customers on the stolen customer list to promote their business Club 88 NY and other business ventures or agreements they had.” (*Id.* ¶ 111.) These conclusory allegations cannot be considered in determining whether Defendants’ proposed counterclaims state a claim for relief. *Iqbal*, 556 U.S. at 678.

Defendants also rely on the fact that the other named Plaintiffs quit Chorus Karaoke on the same day, (Def. Decl. Ex. A ¶ 88), that Hong discussed quitting his employment at Chorus Karaoke with the other named Plaintiffs a week before he quit, (Def. Mem. at 6),² that all of the named Plaintiffs’ names appear on the advertisement for their alleged new business venture, Club 88 NY (Def. Decl. Ex. G), and that Plaintiff HaeYoung Lee organized this business venture. (Def. Decl. Ex. F at 39:14-19). Plaintiffs dispute that the named Plaintiffs all worked at Club 88 NY, that their names appear on its advertisements, and dispute that Plaintiff Jung testified that Plaintiff Haeyong Lee organized the business venture. However, even assuming all of Defendants’ allegations are true, they do not support a conclusion that the other named Plaintiffs conspired with Hong. Defendants do not allege that the other named Plaintiffs had any connection to the alleged unauthorized transfer of Defendants’ proprietary information. Defendants merely allege parallel conduct by the named Plaintiffs, which is not sufficient to

² Defendants cite the transcript of Hong’s deposition for this proposition, but the Court was unable to find support in the transcript. However, even assuming it to be true, Defendants’ counterclaims are futile against the other named Plaintiffs.

establish conspiracy. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556-57 (2007).

Accordingly, Defendants' allegations do not state a claim against the other named Plaintiffs under the CFAA, and Defendants' counterclaim against them would be futile.

2. Defendants' proposed conversion counterclaim is futile

Defendants proposed conversion counterclaim is futile. To state a claim for conversion under New York law, a plaintiff must show that "someone, intentionally and without authority, assume[d] or exercise[d] control over personal property belonging to someone else, interfering with that person's right of possession." *SBIW, Inc. v. Gen. Elec. Co.*, No. 10-CV-7812 (PGG), 2013 WL 5338525 (S.D.N.Y. Sept. 24, 2013), *appeal withdrawn* (Feb. 19, 2014) (quoting *Colavito v. New York Organ Donor Network*, 8 N.Y.3d 43, 49-50 (2006)). "An essential element of conversion is 'unauthorized dominion' to the exclusion of the rights of the plaintiff." *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, 813 F. Supp. 2d 489, 535 (S.D.N.Y. 2011). Defendants have failed to state a claim for conversion because Defendants do not allege that at any point in time they did not have access to the information at issue. *See id.* at 536 (finding plaintiffs failed to state a claim for conversion with respect to a client list when defendant "possessed only a copy of the client list and did not, in any way, limit or otherwise deprive [plaintiffs] of possession or use of that list"). Defendants allege that Hong emailed the files at issue to himself, (Def. Decl. Ex. A ¶ 73), but do not assert that he deleted them from Chorus's business computer. Defendants cite *Thyroff v. Nationwide Mut. Ins. Co.*, 8 N.Y.3d 283, 292-93 (2007), for the proposition that "conversion allows for the full recovery of the value of the intangible property misappropriated even where the property is returned." (Def. Reply In Supp. Of Mot. To Amend ("Def. Reply") at 9.) Defendants' reliance on *Thyroff* is misplaced. The plaintiff in *Thyroff*, unlike Defendants, was deprived of access to his electronic customer

information and personal records. *Thyroff*, 8 N.Y.3d at 285. As the court held in *Geo Grp., Inc. v. Cmty. First Servs., Inc.*, *Thyroff* did “not alter the traditional rule requiring ‘the exercise of unauthorized dominion and control to the complete exclusion of the rightful possessor,’” but rather “simply eliminated the law’s arbitrary distinction between the theft of information stored on a computer and the theft of information printed on paper.” No. 11-CV-1711 (CBA), 2012 WL 1077846, at *9 (E.D.N.Y. Mar. 30, 2012). Accordingly, Defendants’ proposed conversion counterclaim is futile.

3. Defendants’ proposed misappropriation of trade secrets counterclaim is futile.

Defendants’ proposed misappropriation of trade secrets counterclaim is futile. To state a claim for misappropriation of trade secrets, Defendants must allege that 1) Plaintiffs possessed a trade secret, and (2) Plaintiffs used the trade secret “in breach of an agreement, confidential relationship or duty, or as a result of discovery by improper means.” *Faiveley Transport Malmo AB v. Wabtec Corp.*, 559 F.3d 110, 117 (2d Cir. 2009) (internal quotation marks omitted). Defendants allege that: 1) “Plaintiffs used the Chorus proprietary information that they conspired to steal from Defendants to promote their new financial venture at Club 88 NY” (Def. Decl. Ex. A ¶ 90); 2) “Plaintiffs sold the subject customer list to third parties and unjustly enriched themselves” (*Id.* ¶ 105); 3) “Plaintiffs in this action aided and abetted Plaintiff Hong in the theft of the Defendants’ e-files and knowingly misappropriated and used or misused its exclusive proprietary information including trade secrets, financial information, customer lists, customer financial information and other employees’ personal and financial information for Plaintiffs’ legal and pecuniary benefit” (*Id.* ¶ 110); and 4) “Plaintiffs contacted or solicited customers on the stolen customer list to promote their business Club 88 NY and other business ventures or agreements they had” (*Id.* ¶ 111). Despite Defendants’ bold assertions, Defendants put forward

no information or evidence to suggest that any of the allegedly stolen information falls into the category of “trade secrets.” Defendants’ allegations regarding Plaintiffs’ use of trade secrets are thus conclusory. *Iqbal*, 556 U.S. at 678. Defendants do not assert any details regarding in what ways Plaintiffs allegedly misused the customer list, nor do they identify any customers who were supposedly contacted or solicited, nor any other business ventures or agreements Plaintiffs had. Accordingly, Defendants’ proposed misappropriation of trade secrets claim is futile.

4. Defendants’ unjust enrichment claim is futile.

The elements of an unjust enrichment claim are: “1) defendant was enriched, 2) at plaintiff’s expense, and 3) equity and good conscience militate against permitting defendant to retain what plaintiff is seeking to recover.” *Briarpatch Ltd., L.P. v. Phoenix Pictures, Inc.*, 373 F.3d 296, 306 (2d Cir. 2004). Defendants allege that: 1) “Plaintiffs unjustly enriched themselves with any profits made from the stolen proprietary information taken from Chorus’ business computer” (Def. Decl. Ex. A ¶ 117); and 2) “Even if the proprietary information is returned to the Defendants, it does not make Defendants financially whole and it is against equity and good conscience to allow Plaintiffs to retrain the benefits derived from their wrongful conduct.” Defendants do not allege any facts to support the counterclaim, other than conclusory allegations that merely restate the elements of unjust enrichment. *Iqbal*, 556 U.S. at 678. Therefore, Defendants’ counterclaim for unjust enrichment is futile.

IV. CONCLUSION

For the foregoing reasons, Defendants’ motion to amend is **DENIED** pursuant to Rule 16(b) for failure to demonstrate good cause, and, alternatively is **DENIED** pursuant to Rule 15(a) for undue delay. However, even if Defendants demonstrated good cause and did not act with undue delay, Defendants’ proposed conversion, misappropriation of trade secrets, and

unjust enrichment counterclaims and Defendants' proposed CFAA counterclaim against Plaintiffs Hyo Jung, JeongMin Song, HaeYong Lee, Dal Young Cho, Kyungmo Yan, and SangYoon Shin would be futile, and therefore the motion to amend should be **DENIED** with respect to those claims under Rule 15(a). Defendants proposed CFAA counterclaim against Plaintiff Hong would not be futile, but does not provide a compelling basis for reconsidering the Rule 16(b) determination.

DATED: September 11, 2014
New York, New York

Respectfully Submitted,

A handwritten signature in black ink, appearing to read "Ronald L. Ellis", written over a horizontal line.

The Honorable Ronald L. Ellis
United States Magistrate Judge

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

HILARY REMIJAS, MELISSA FRANK,
DEBBIE FARNOUSH, and JOANNE KAO,
individually and on behalf of all others
similarly situated,

Plaintiff,

v.

THE NEIMAN MARCUS GROUP, LLC, a
Delaware limited liability company,

Defendant.

No. 14 C 1735
Judge James B. Zagel

MEMORANDUM OPINION AND ORDER

Plaintiffs Hilary Remijas, Melissa Frank, Debbie Farnoush, and Joanne Kao, individually and on behalf of all others similarly situated, have brought this action against Defendant Neiman Marcus for negligence, breach of implied contract, unjust enrichment, unfair and deceptive business practices, invasion of privacy, and violation of several state data breach acts. Defendant now moves to dismiss pursuant to Fed.R.Civ.P. 12(b)(1) for lack of Article III standing, and pursuant to Fed.R.Civ.P. 12(b)(6) for failure to state a claim. For the following reasons, Defendant's motion to dismiss is granted for lack of standing.

BACKGROUND

Defendant is a high-end department store. In 2013, hackers breached Defendant's servers, resulting in the potential disclosure of 350,000 customers' payment card data and personally identifiable information. At some point following the breach, it became clear that, of the payment cards that may have been affected, at least 9,200 were subsequently used fraudulently elsewhere. Plaintiffs are among the 350,000 customers, and they have brought this

lawsuit against Defendant for failing to adequately protect against such a security breach, and for failing to provide timely notice of the breach once it happened.

Plaintiffs assert that they have been injured in that Defendant's alleged misconduct exposed them to an increased risk of future fraudulent credit card charges, and an increased risk of identity theft. Plaintiffs also assert present injuries, including the loss of time and money associated with resolving fraudulent charges, the loss of time and money associated with protecting against the risk of future identity theft, the financial loss they suffered from having purchased products that they wouldn't have purchased had they known of Defendant's misconduct, and the loss of control over and value of their private information. Defendant argues that none of these asserted injuries is sufficient to establish Article III standing.

DISCUSSION

It is a plaintiff's burden to establish Article III standing. *Apex Digital, Inc. v. Sears, Roebuck, & Co.*, 572 F.3d 440, 443 (7th Cir. 2009). This requires the plaintiff to demonstrate: (1) an "injury in fact" that is concrete and particularized and either actual or imminent; (2) that the injury is fairly traceable to the challenged action by the defendant; and (3) that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1147 (2013). Because standing is not a mere pleading requirement, but rather an indispensable part of the plaintiff's case, it must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, i.e., with the manner and degree of evidence required at the successive stages of the litigation. *Apex Digital*, 572 F.3d at 443. Plaintiffs assert four principal categories of injury. I address each in turn.

A. The Increased Risk of Future Harm

Allegations of future potential harm may suffice to establish Article III standing, but the

future harm must be “certainly impending.” *See Clapper*, 133 S.Ct. at 1147 (collecting cases). Three courts in this District have recently taken up the question of standing and the increased risk of future harm plaintiffs encounter in the context of such cyber-attacks. *See Moyer v. Michaels Stores, Inc.*, 2014 WL 3511500 (N.D.Ill. July 14, 2014); *Strautins v. Trustwave Holdings, Inc.*, 2014 WL 960816 (N.D.Ill. March 12, 2014); *In re Barnes & Noble Pin Pad Litigation*, 2013 WL 4759588 (N.D.Ill. Sept. 3, 2013).

The courts in *Strautins* and *Barnes & Noble* both held that the alleged increased risk of future harm was insufficient to establish standing. Defendant argues that this case is like *Strautins* and *Barnes & Noble*. In *Moyer*, the Court held that the alleged increased risk of future harm was sufficient to establish standing, but Defendant contends that this holding was premised on a misreading of relevant case law, and it should not be followed. The differing outcomes in *Strautins* and *Barnes & Noble* on the one hand, and *Moyer* on the other are in part attributable to conflicting readings of the Supreme Court’s recent decision in *Clapper*.

The *Strautins* Court concluded that *Clapper* implicitly overruled a facially more relaxed standard for evaluating standing in this context articulated in *Pisciotta v. Old Nat. Bancorp.*, 499 F.2d 629, 634 (7th Cir. 2007). In *Pisciotta*, the Court held that “the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions.” *Id.* The *Strautins* Court held that, by emphasizing the “certainly impending” standard, the Supreme Court “seems rather plainly to reject the premise, implicit in *Pisciotta* [], that any marginal increase in risk is sufficient to confer standing.” *Strautins*, 2014 WL 960816, at *5. The *Barnes & Noble* Court relied on *Clapper*’s “certainly impending” analysis without reference to *Pisciotta*.

The *Moyer* Court, by contrast, understood *Clapper* to have applied a particularly rigorous standing analysis to a claim that particularly called for it – a claim that implicated the actions of the political branches of government in the fields of intelligence gathering and foreign affairs, and that argued that an action taken by one of the other two branches of the federal government was unconstitutional. *See Moyer*, 2014 WL 3511500, at *5; *see also Strautins*, 2014 WL 960816, at *5 n. 11. These cyber-attack/credit card cases implicate neither questions of national security nor the constitution. The *Moyer* Court concluded that there was room for *Clapper* and *Pisciotta* to co-exist. *See Moyer*, 2014 WL 3511500, at *6.

For my part, I note that the “certainly impending” standard pre-dates *Clapper*, *see Babbitt v. Farm Workers*, 442 U.S. 289, 298 (1979), though I also note that the *Clapper* Court itself acknowledged that the underlying facts called for an “especially rigorous” standing inquiry, *see Clapper*, 133 S.Ct. at 1147. Those facts are not present here. Read literally, *Pisciotta* could be understood to have held that *any* marginal increase in the risk of future injury is sufficient to confer Article III standing. That would be difficult to square with *Clapper*, which sets a threshold that an increase in the risk of harm must meet in order to confer standing. *Id.* But in my view, it is hard to imagine that that is what the *Pisciotta* Court intended, and such a literal reading of *Pisciotta* would not be reasonable. The *Pisciotta* Court raised the issue of standing *sua sponte*, and was not prompted to thoroughly discuss it. Though it does not expressly say so, *Pisciotta* was constrained by the “certainly impending” standard, first articulated 27 years earlier in *Babbitt*, and I read that standard into the opinion.

Legal standards aside, the underlying facts in *Pisciotta*, *Strautins*, *Barnes & Noble*, and the instant case materially differ with respect to standing. First, in *Pisciotta*, it appears as though the plaintiffs’ data were actually stolen (at the very least, the Court’s analysis assumed as much).

See Pisciotta, 499 F.3d at 634. At issue with respect to the plaintiffs' injury, then, was whether and how likely the stolen data would actually be misused. *Id.* This is distinct from *Strautins* and *Barnes & Noble*, where the respective Courts found that the plaintiffs had alleged merely that there was a *possibility* that their data had been stolen. *See Strautins*, 2014 WL 960816, at *4, *6; *Barnes & Noble*, 2013 WL 4759588, at *4. Compared to the facts in *Pisciotta*, the fact that any given plaintiff's data may not have even been stolen yielded a much weaker inference that the data were actually at a sufficiently increased risk of being misused. In my view, this is a principled distinction that could justify holding that *Pisciotta* satisfied the "certainly impending" standard (albeit under a less rigorous application of the standard outside the national security/constitutional context) while holding that *Strautins* and *Barnes & Noble* did not.

The facts in the instant case present a third permutation. Here, the overwhelming majority of the plaintiffs allege only that their data *may* have been stolen. In this sense, the instant case is like *Strautins* and *Barnes & Noble*. Unlike *Strautins* and *Barnes & Noble*, however, Plaintiffs also allege (and Defendant acknowledges) that 9,200, or approximately 2.5% of these customers have actually had fraudulent charges appear on their credit cards. In other words, these customers' data were actually stolen and were actually misused. This allegation permits several inferences of varying strength with respect to Plaintiffs' claims to standing.

First, it certainly permits the inference that these 9,200 customers did indeed have their data stolen as a result of the cyber-attack on Defendant. That is an injury in fact, the sufficiency of which for purposes of standing will be addressed below. Second, it permits a weaker, though in my view still plausible, inference that others among the 350,000 customers are at a "certainly impending" risk of seeing similar fraudulent charges appear on their credit cards as a result of the cyber-attack on Defendant. The significance of that potential future injury for purposes of

standing will also be discussed below. I do not believe, however, that this allegation permits a plausible inference that any of the 350,000 customers are at a “certainly impending” risk of the other future injury claimed by Plaintiffs – identity theft.

It is not clear to me that the “fraudulent charge” injury alleged to have been incurred by the 9,200 customers, or, *a fortiori*, the risk that the same injury may befall others among the 350,000 customers at issue, is an injury sufficient to confer standing. To satisfy their burden to establish standing, plaintiffs must show that their injury is concrete, particularized, and, if not actual, at least imminent. *See Clapper*, 133 S.Ct. at 1147. As discussed above, I am satisfied that the potential future fraudulent charges are sufficiently “imminent” for purposes of standing. But of course, even having conceded imminence, both injuries (present and future) must still be concrete. Here, as common experience might lead one to expect, Plaintiffs have not alleged that any of the fraudulent charges were unreimbursed. On these pleadings, I am not persuaded that unauthorized credit card charges for which none of the plaintiffs are financially responsible qualify as “concrete” injuries. *See Barnes & Noble*, 2013 WL 4759588, at *6; *Hammond v. Bank of N.Y. Mellon Corp.*, 2010 WL 2643307, *8 (S.D.N.Y. June 25, 2010). Without a more detailed description of some fairly substantial attendant hardship, I cannot agree with Plaintiffs that such “injuries” confer Article III standing.

Next, as noted above, I am not persuaded that the 350,000 customers at issue are at a certainly impending risk of identity theft. Unlike the *Pisciotta* plaintiffs, the plaintiffs here do not allege that data belonging to all of the customers at issue were in fact stolen. They allege that approximately 2.5% of the customers at issue saw fraudulent charges on their credit cards, supporting a strong inference that *those* customers’ data were stolen as a result of Defendant’s data breach. And again, I accept the inference from this that additional customers are at a

“certainly impending” risk of future fraudulent charges on their credit cards. But to assert on this basis that either set of customers is also at a certainly impending risk of identity theft is, in my view, a leap too far.¹ The complaint does not adequately allege standing on the basis of increased risk of future identity theft.

B. Time and Money Spent to Mitigate the Risk of Future Fraud and Identity Theft

Plaintiffs also claim the time and money allegedly spent toward mitigating the risk of future fraudulent charges and identity theft constitutes injury sufficient to confer standing. The cost of guarding against a risk is an injury sufficient to confer standing only if the underlying harm the plaintiff is seeking to avoid is itself a cognizable Article III injury. *See Moyer*, 2014 WL 3511500, at *4 n. 1. As discussed above, however, on these pleadings I am not satisfied that either of the future injuries claimed in the complaint are themselves sufficient to confer standing.

The “fraudulent charge” injury, absent unreimbursed charges or other allegations of some substantial attendant hardship, is not in my view sufficiently concrete to establish standing. In any event, the complaint contains no meaningful allegations as to what precisely the costs incurred to mitigate the risk of future fraudulent charges were. Generally, when one sees a fraudulent charge on a credit card, one is reimbursed for the charge, and the threat of future charges is eliminated by the issuance of a new card, perhaps resulting in a brief period where one is without its use. If the complaint is to credibly claim standing on this score, it must allege something that goes beyond such *de minimis* injury.

As discussed above, the complaint does not adequately allege that the risk of identity theft is sufficiently imminent to confer standing. So long as that is the case, the “time and money

¹ I note that one plaintiff allegedly received a “phishing” phone call as a result of the cyber-attack on Defendant which, if she had disclosed private information, might have led to future identity theft. In my view, this allegation is sufficient neither to establish a “certainly impending” risk of identity theft, nor to qualify as a “concrete” injury for purposes of standing.

spent to mitigate” claim as to the risk of identity theft, which may well be more substantial than the same claim as to the risk of fraudulent credit card charges, is not a cognizable Article III injury.

C. The Financial Injury For Having Purchased Defendant’s Products

Plaintiffs also assert that they paid a premium for the retail goods purchased at Defendant’s stores, a portion of which Defendant was required to allocate to adequate data breach security measures. Because Defendant did not do so, Plaintiffs allege, Plaintiffs overpaid for their respective purchases and would not have otherwise made them. As Plaintiffs would have it, this financial injury establishes standing.

The argument is creative, but unpersuasive. All of the cases to which Plaintiffs cite in support of this proposition involved products which possessed some sort of deficiency. Plaintiffs purchased bottled water and it turned out to be municipal tap water. *Chicago Faucet Shoppe, Inc. v. Nestle Waters N. Am Inc.*, 2014 WL 541644, *3 (N.D.Ill. Feb. 11, 2014). Plaintiffs purchased children’s toys and they turned out to be toxic. *In re Aqua Dots Prods. Liab. Litig.*, 654 F.3d 748, 751 (7th Cir. 2011). As the Seventh Circuit noted, the fact that members of the class in such a case did not suffer physical injury did not mean that they were not injured. “The plaintiffs’ loss is financial: they paid more for the toys [or water] than they would have.” *Id.*

In my view, a vital limiting principle to this theory of injury is that the value-reducing deficiency is always intrinsic to the product at issue. Under Plaintiffs’ theory, however, the deficiency complained of is extrinsic to the product being purchased. To illustrate the problem this creates: suppose a retail store does not allocate a sufficient portion of its revenues to providing adequate in-store security. A customer who is assaulted in the parking lot after patronizing the store may well have a negligence claim against the store owner. But could he or

she really argue that she overpaid for the products that she purchased? Or even more to the point: even if no physical injury actually befell the customer, under Plaintiffs' theory, the customer still suffered financial injury because he or she paid a premium for adequate store security, and the store security was not in fact adequate.

As set forth in *Aqua Dots*, this theory of injury is plainly sensible. In my view, however, expanding it to include deficiencies extrinsic to the purchased product would effectively render it meaningless.

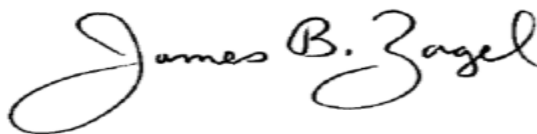
D. The Loss of Control Over and Value of Plaintiffs' Private Information

Finally, I am also unpersuaded by Plaintiffs' claim to standing based on the loss of control over and value of their private information. Again, the injury as pled is not sufficiently concrete. *Cf. Barnes & Noble*, 2013 WL 4759588 (no actual injury of this sort where plaintiffs do not allege that their personal information was sold or that the plaintiffs themselves could have sold it).

CONCLUSION

For the foregoing reasons, Defendant's motion to dismiss for lack of Article III standing is granted.

ENTER:

A handwritten signature in black ink that reads "James B. Zagel". The signature is written in a cursive, flowing style with a large initial "J".

James B. Zagel
United States District Judge

DATE: September 16, 2014

NOTICE: This opinion is subject to formal revision before publication in the bound volumes of NLRB decisions. Readers are requested to notify the Executive Secretary, National Labor Relations Board, Washington, D.C. 20570, of any typographical or other formal errors so that corrections can be included in the bound volumes.

**Three D, LLC d/b/a Triple Play Sports Bar and Grille
and Jillian Sanzone**

**Three D, LLC d/b/a Triple Play Sports Bar and Grille
and Vincent Spinella. Cases 34–CA–012915 and
34–CA–012926**

August 22, 2014

DECISION AND ORDER

BY MEMBERS MISCIMARRA, HIROZAWA,
AND SCHIFFER

The principal issue in this case is whether the Respondent violated Section 8(a)(1) of the Act by discharging two employees for their participation in a Facebook discussion involving claims that employees unexpectedly owed additional State income taxes because of the Respondent's withholding mistakes.¹ We agree with the judge that the discharges were unlawful. We also adopt the judge's findings that the Respondent violated the Act by threatening employees with discharge for and interrogating employees about their Facebook activity, as well as by informing employees they were being discharged

¹ On January 3, 2012, Administrative Law Judge Lauren Esposito issued the attached decision. The General Counsel and the Respondent each filed exceptions, a supporting brief, and an answering brief to the other party's exceptions.

The National Labor Relations Board has delegated its authority in this proceeding to a three-member panel.

The Board has considered the decision and the record in light of the exceptions and briefs and has decided to affirm the judge's rulings, findings, and conclusions only to the extent consistent with this Decision and Order. We have amended the judge's conclusions of law consistent with our findings herein. We have amended the remedy and modified the judge's recommended Order consistent with our legal conclusions herein, and we shall substitute a new notice to conform to the Order as modified and in accordance with our decision in *Durham School Services*, 360 NLRB No. 85 (2014). In addition to the remedies recommended by the judge, we shall order the Respondent to compensate Charging Parties Jillian Sanzone and Vincent Spinella for the adverse tax consequences, if any, of receiving lump-sum backpay awards, and to file a report with the Social Security Administration allocating the backpay awards to the appropriate calendar quarters for each employee. We shall also modify the judge's recommended Order in accordance with our decision in *Guardsmark, LLC*, 344 NLRB 809, 812 (2005), *enfd.* in relevant part 475 F.3d 369 (D.C. Cir. 2007).

The Respondent has implicitly excepted to some of the judge's credibility findings. The Board's established policy is not to overrule an administrative law judge's credibility resolutions unless the clear preponderance of all the relevant evidence convinces us that they are incorrect. *Standard Dry Wall Products*, 91 NLRB 544 (1950), *enfd.* 188 F.2d 362 (3d Cir. 1951). We have carefully examined the record and find no basis for reversing the judge's findings.

because of their Facebook activity.² In addition, we adopt the judge's finding that the Respondent unlawfully threatened legal action for engaging in that activity.³ Finally, we reverse the judge and find that the Respondent violated Section 8(a)(1) by maintaining its "Internet/Blogging" policy. We address in detail the discharges, then the policy.

I.

Section 7 of the National Labor Relations Act provides, in pertinent part, that "[e]mployees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection" Under Section 7, employees have a statutory right to act together "to improve terms and conditions of employment or otherwise improve their lot as employees"⁴—including by using social media to communicate with each other and with the public for that purpose. At the same time, online employee communications can implicate legitimate employer interests, including the "right of employers to maintain discipline in their establishments."⁵ However,

² We agree with the judge that the Respondent separately violated Sec. 8(a)(1) of the Act by telling Sanzone and Spinella that their Facebook activity was the reason for their discharges. In doing so, we rely on *Benesight, Inc.*, 337 NLRB 282, 283–284 (2001) (finding statement to employee linking her unlawful discharge to her protected activity independently violated Sec. 8(a)(1) separate and apart from the discharge itself). We do not rely on the cases cited by the judge—*Extreme Building Services Corp.*, 349 NLRB 914, 914 fn. 3 (2007); *Watts Electric Corp.*, 323 NLRB 734, 735 (1997), *revd.* in part, vacated in part *mem.* 166 F.3d 351 (11th Cir. 1998)—which involved employers unlawfully telling employees that *another* employee had been discharged for engaging in protected activities.

³ In adopting the judge's finding that the Respondent unlawfully threatened legal action, we rely on the Respondent's postdischarge statement to Spinella that he would "be hearing from [the Respondent's] lawyers." The threat directed at Spinella was not incidental to a lawsuit: the Respondent's counsel did not contact Spinella and the Respondent took no legal action against him. Accordingly, by its threat, the Respondent violated Sec. 8(a)(1) of the Act, regardless of whether a lawsuit against Spinella would have been unlawful had one been filed. See *DHL Express, Inc.*, 355 NLRB 680, 680 fn. 3 (2010). The judge erred in stating that the Board has "explicitly declined to apply" the principles of *BE & K Construction Co.*, 351 NLRB 451 (2007), to threats to initiate litigation "where they are 'incidental' to the actual filing of the lawsuit itself." That issue remains undecided. See *DHL Express, Inc.*, *supra* at 680 fn. 3; *Postal Service*, 350 NLRB 125, 126 fn. 5 (2007), *enfd.* 526 F.3d 729 (11th Cir. 2008). We need not resolve it here. We find it unnecessary to pass on the judge's finding that the Respondent also violated Sec. 8(a)(1) by threatening Sanzone with legal action because finding that additional violation would be cumulative and would not affect the remedy.

⁴ *Valley Hospital Medical Center*, 351 NLRB 1250, 1252 (2007), *enfd.* 358 Fed. Appx. 783 (9th Cir. 2009).

⁵ *Republic Aviation Corp. v. NLRB*, 324 U.S. 793, 798 (1945).

neither of these rights is “unlimited in the sense that [it] can be exercised without regard to any duty which the existence of rights in others may place upon employer or employee.”⁶ In this case, there is no dispute that the Facebook communications at issue constituted “concerted activities” and that they were “for the purpose of . . . mutual aid or protection.” Rather, mindful of the balance to be struck between employee rights under Section 7 and legitimate employer interests, our focus here is on whether these Facebook activities, which indisputably prompted the Respondent to discharge the two employees, lost the protection of the Act. While our analysis differs somewhat from that of the judge, we agree that they did not.

A.

The Respondent, which is owned by Ralph DelBuono and Thomas Daddona, operates a bar and restaurant; DelBuono is responsible for the Respondent’s accounting. The Respondent’s employees are not represented by a labor organization.

The Respondent employed Jillian Sanzone as a waitress and bartender, and Vincent Spinella as a cook. In approximately January 2011,⁷ Sanzone and at least one other employee discovered that they owed more in State income taxes than they had expected. Sanzone discussed this at work with other employees, and some employees complained to the Respondent. In response to the complaints, the Respondent planned a staff meeting for February with its payroll provider to discuss the employees’ concerns.

Sanzone, Spinella, and former employee Jamie LaFrance, who left the Respondent’s employ in November 2010, have Facebook accounts. On January 31, LaFrance posted the following “status update” to her Facebook page:

Maybe someone should do the owners of Triple Play a favor and buy it from them. They can’t even do the tax paperwork correctly!!! Now I OWE money...Wtf!!!!

The following comments were posted to LaFrance’s page in response:⁸

KEN DESANTIS (a Facebook “friend” of LaFrance’s and a customer): “You owe them money...that’s fucked up.”

DANIELLE MARIE PARENT (Triple Play employee): “I FUCKING OWE MONEY TOO!”

⁶ Ibid.

⁷ All dates are in 2011, unless otherwise noted.

⁸ We quote the comments verbatim without the corrections the judge made in her decision.

LAFRANCE: “The state. Not Triple Play. I would never give that place a penny of my money. Ralph [DelBuono] fucked up the paperwork...as per usual.”

DESANTIS: “yeah I really dont go to that place anymore.”

LAFRANCE: “It’s all Ralph’s fault. He didn’t do the paperwork right. I’m calling the labor board to look into it bc he still owes me about 2000 in paychecks.”

(At this juncture, employee Spinella selected the “Like” option under LaFrance’s initial status update. The discussion continued as follows.)

LAFRANCE: “We shouldn’t have to pay it. It’s every employee there that its happening to.”

DESANTIS: “you better get that money...thats bullshit if thats the case im sure he did it to other people too.”

PARENT: “Let me know what the board says because I owe \$323 and ive never owed.”

LAFRANCE: “I’m already getting my 2000 after writing to the labor board and them investigating but now I find out he fucked up my taxes and I owe the state a bunch. Grrr.”

PARENT: “I mentioned it to him and he said that we should want to owe.”

LAFRANCE: “Hahahaha he’s such a shady little man. He prolly pocketed it all from all our paychecks. I’ve never owed a penny in my life till I worked for him. Thank goodness I got outta there.”

SANZONE: “I owe too. Such an asshole.”

PARENT: “yeah me neither, i told him we will be discussing it at the meeting.”

SARAH BAUMBACH (Triple Play employee): “I have never had to owe money at any jobs...i hope i wont have to at TP...probably will have to seeing as everyone else does!”

LAFRANCE: “Well discuss good bc I won’t be there to hear it. And let me know what his excuse is ;).”

JONATHAN FEELEY (a Facebook “friend” of LaFrance’s and customer): “And ther way to expensive.”

Sanzone added her comment from her cell phone on February 1. She testified that her Facebook privacy settings permit only her Facebook friends to view her posts.⁹ LaFrance’s privacy settings are not in the record.

Co-owner Daddona learned about the Facebook discussion from his sister, who, in addition to being em-

⁹ To become Facebook “friends,” one person must send a “friend request,” and the recipient must accept the request.

ployed by the Respondent, is a Facebook friend of LaFrance. On February 2, when Sanzone reported to work, Daddona told her she was being discharged. When Sanzone asked why, Daddona responded that she was not loyal enough to be working for the Respondent because of her Facebook comment.

When Spinella reported for work on February 3, he was summoned to the Respondent's office, where Daddona and DelBuono were waiting; the Facebook comments from LaFrance's account were displayed on a computer screen in the office. After asking Spinella if he "had a problem with them, or the company," DelBuono and Daddona interrogated him about the Facebook discussion, the meaning of his "Like" selection, the identity of the other people who had participated in the conversation, and whether Spinella had written anything negative about DelBuono or Daddona. DelBuono told Daddona that the "Like" option meant that Spinella stood behind the other commenters. He told Spinella that, because he "liked the disparaging and defamatory comments," it was "apparent" that Spinella wanted to work somewhere else. DelBuono also said that his attorney had informed him that he should discharge anyone involved in the Facebook conversation for defamation. DelBuono then discharged Spinella. As Spinella was leaving, DelBuono said, "You'll be hearing from our lawyers." The Respondent's counsel did not contact Spinella, and the Respondent did not take any legal action against him. Counsel did contact Sanzone by letter, raising the possibility of an action for defamation. Counsel also contacted LaFrance, who thereafter deleted the entire conversation and posted a retraction.

B.

The judge found that the Facebook discussion was *concerted* activity because it involved four current employees (Danielle Marie Parent, Sarah Baumbach, Sanzone, Spinella) and was "part of an ongoing sequence" of discussions that began in the workplace about the Respondent's calculation of employees' tax withholding. Noting that the employees, in their Facebook conversation, discussed issues they intended to raise at an upcoming staff meeting as well as possible avenues for complaints to government entities, the judge found that the participants were seeking to initiate, induce, or prepare for group action. As a result, the judge concluded that the Facebook discussion was concerted under the standard set forth in *Meyers Industries*, 281 NLRB 882, 887 (1986).¹⁰

¹⁰ Enfd. sub nom. *Prill v. NLRB*, 835 F.2d 1481 (D.C. Cir. 1987), cert. denied 487 U.S. 1205 (1988).

The judge further found that Sanzone and Spinella were engaged in *protected* concerted activity because the discussion concerned workplace complaints about tax liabilities, the Respondent's tax withholding calculations, and LaFrance's assertion that she was owed back wages. The judge found that Spinella's selection of the "Like" button expressed his support for the others who were sharing their concerns and "constituted participation in the discussion that was sufficiently meaningful as to rise to the level of" protected, concerted activity. Having found Sanzone's and Spinella's Facebook activities protected by the Act, the judge further found that they did not lose the Act's protection under the test set forth in *Atlantic Steel Co.*, 245 NLRB 814 (1979), or under the standards established in *NLRB v. Electrical Workers Local 1229 (Jefferson Standard)*, 346 U.S. 464 (1953), and *Linn v. Plant Guards Local 114*, 383 U.S. 53 (1966). Applying *NLRB v. Burnup & Sims*, 379 U.S. 21 (1964), and *Wright Line*, 251 NLRB 1083 (1980),¹¹ the judge concluded that the Respondent unlawfully discharged Sanzone and Spinella for their protected Facebook posts.

C.

The Respondent does not dispute that the employees' Facebook activity was concerted or that its employees have a protected right to engage in a Facebook discussion about the Respondent's tax withholding calculations that looks toward group action. Rather, citing *Linn*, *Jefferson Standard*, and *Atlantic Steel*, it contends that, as a result of their Facebook activities, Sanzone and Spinella adopted LaFrance's allegedly defamatory and disparaging comments and lost the protection of the Act.¹² The Respondent asserts that the Facebook posts were made in a "public" forum accessible to both employees and customers and that, as a result, they undermined DelBuono's authority in the workplace and adversely affected the Respondent's public image. Finally, the Respondent contends that *NLRB v. Burnup & Sims*, 379 U.S. at 21, cited by the judge, is inapplicable here.

D.

We begin by finding that, as a general matter, the *Atlantic Steel* framework is not well suited to address issues that arise in cases like this one involving employees' off-duty, offsite use of social media to communicate with other employees or with third parties. As a result, we do not follow the judge's lead in applying *Atlantic Steel* to determine whether Sanzone's and Spinella's Fa-

¹¹ Enfd. 662 F.2d 899 (1st Cir. 1981), cert. denied 455 U.S. 989 (1982).

¹² The Respondent further maintains that it lawfully discharged Spinella for performance problems.

cebook comments lost the protection of the Act. Rather, we assess their comments under *Jefferson Standard* and *Linn*, concluding that under those decisions, the comments were statutorily protected. Applying the well-established *Wright Line* test, in turn, we conclude that the discharges of Sanzone and Spinella were unlawful.

1.

To determine whether an employee loses the Act's protection under *Atlantic Steel*, the Board balances four factors: (1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee's outburst; and (4) whether the outburst was, in any way, provoked by the employer's unfair labor practices. This multifactor framework enables the Board to balance employee rights with the employer's interest in maintaining order at its workplace. See *Plaza Auto Center, Inc.*, 355 NLRB 493, 494 (2010), *enfd.* in part 664 F.3d 286 (9th Cir. 2011), decision on remand 360 NLRB No. 117 (2014). Typically, the Board has applied the *Atlantic Steel* factors to analyze whether direct communications, face-to-face in the workplace, between an employee and a manager or supervisor constituted conduct so opprobrious that the employee lost the protection of the Act. *Atlantic Steel* generally has not been applied to communications by employees with third parties or the general public. See, e.g., *Valley Hospital Medical Center*, supra, 351 NLRB at 1252, *enfd.* sub nom. *Nevada Service Employees Local 1107 v. NLRB*, 358 Fed.Appx. 783 (9th Cir. 2009); *Emarco, Inc.*, 284 NLRB 832, 833 (1987). Rather, in those cases, the Board has applied the standards set forth in *Jefferson Standard* and *Linn*.¹³

The clear inapplicability of *Atlantic Steel*'s "place of the discussion" factor supports our conclusion that the *Atlantic Steel* framework is tailored to workplace confrontations with the employer.¹⁴ We do not suggest that

¹³ We disagree with our dissenting colleague's assertion that the Board's decision in *Restaurant Horikawa*, 260 NLRB 197, 198 (1982), sets forth the applicable standard for deciding whether a retail employee who engages in misconduct in the presence of customers loses the protection of the Act. See *Starbucks Coffee Co.*, 360 NLRB No. 134, slip op. at 2 fn. 10 (2014).

¹⁴ The Board has applied *Atlantic Steel* to confrontational verbal attacks on supervisors that occurred near, but not within, the workplace. See, e.g., *Starbucks Coffee Co.*, 354 NLRB 876 (2009) (finding that employee lost protection when she followed, taunted, and intimidated a manager after a union rally outside the employer's coffee shop), adopted in 355 NLRB 636 (2010), *enf. denied* in part, and remanded on other grounds sub nom. 679 F.3d 70 (2d Cir. 2012), decision on remand *Starbucks*, supra, 360 NLRB No. 134. The *Starbucks* Board stated that the location of an employee's misconduct weighs against protection when the employee engages in insubordinate or profane conduct toward a supervisor in front of other employees, regardless of whether those employees are on or off-duty. But there the confrontation began in front of the employer's store following an employer-sponsored event,

employees' off-duty, offsite use of social media can never implicate an employer's interest in maintaining workplace discipline and order in the same manner that a face-to-face workplace confrontation with a manager or supervisor does. Here, however, we find that the *Atlantic Steel* framework is particularly inapplicable. The employees engaged in protected concerted activity by taking part in a social media discussion among offsite, off-duty employees, as well as two nonemployees.¹⁵ No manager or supervisor participated in the discussion, and there was no direct confrontation with management.¹⁶ Although we do not condone her conduct, we find that Sanzone's use of a single expletive to describe a manager, in the course of a protected discussion on a social media website, does not sufficiently implicate the Respondent's legitimate interest in maintaining discipline and order in the workplace to warrant an analysis under *Atlantic Steel*.¹⁷

2.

Having found that *Atlantic Steel* does not apply here, we must next consider whether the Facebook activities of Sanzone or Spinella lost the protection of the Act under precedent relating to disloyal or defamatory statements.

The Board has long recognized that an employer has a legitimate interest in preventing the disparagement of its products or services and, relatedly, in protecting its reputation (and the reputations of its agents as to matters within the scope of their agency) from defamation. Section 7 rights are balanced against these interests, if and when they are implicated. In striking that balance, the

in the presence of employees under the manager's authority. 354 NLRB at 878. The exceptional circumstances of that case confirm that *Atlantic Steel* typically applies to workplace confrontations.

¹⁵ We reject the Respondent's contention that Sanzone's conduct lost the Act's protection because her Facebook comment was visible to customers Ken DeSantis and Jonathan Feeley. DeSantis and Feeley joined the discussion as LaFrance's Facebook friends on their own initiative and in the context of a social relationship with LaFrance outside of the workplace, not because they were the Respondent's customers. This off-duty discussion away from the Respondent's premises did not disrupt any customer's visit to the Respondent. And, as discussed below, the employee disloyalty perceived by the Respondent did not deprive Sanzone of the Act's protection.

¹⁶ In all likelihood, the revelation at their termination meetings that the Respondent had seen the Facebook comments came as a complete, and unwelcome, surprise to both Spinella and Sanzone.

¹⁷ Indeed, an employee does not necessarily lose the protection of the Act by impulsively directing profanity at supervisors in the course of otherwise-protected activity. Compare *Great Dane Trailers*, 293 NLRB 384, 384, 393 (1989) (employee did not lose protection for calling his foreman a "fucked up foreman" on the shop floor after employee's requests for assistance were denied), with *DaimlerChrysler Corp.*, 344 NLRB 1324, 1329 (2005) (no protection for sustained, profane, ad hominem attack on supervisor in work area during worktime).

Board applies these principles in accordance with the Supreme Court's decisions in *Jefferson Standard* and *Linn*.

In *Jefferson Standard*, the Court upheld the discharge of employees who publicly attacked the quality of their employer's product and its business practices without relating their criticisms to a labor controversy. The Court found that the employees' conduct amounted to disloyal disparagement of their employer and, as a result, fell outside the Act's protection. 346 U.S. at 475–477.

In *Linn*, the Court limited the availability of State-law remedies for defamation in the course of a union organizing campaign “to those instances in which the complainant can show that the defamatory statements were circulated with malice and caused him damage.” 383 U.S. at 64–65. The Court indicated that the meaning of “malice,” for these purposes, was that the statement was uttered “with knowledge of its falsity, or with reckless disregard of whether it was true or false.” *Id.* at 61.

Applying these precedents, the Board has held that “employee communications to third parties in an effort to obtain their support are protected where the communication indicated it is related to an ongoing dispute between the employees and the employers and the communication is not so disloyal, reckless, or maliciously untrue as to lose the Act's protection.” *MasTec Advanced Technologies*, 357 NLRB No. 17, slip op. at 5 (2011) (quoting *Mountain Shadows Golf Resort*, 330 NLRB 1238, 1240 (2000)).

Turning to the facts of this case, we first adopt the judge's finding that the only employee conduct to be analyzed is Sanzone's comment (“I owe too. Such an asshole.”) and Spinella's indication that he “liked” LaFrance's initial status update (“Maybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money...Wtf!!!!”). In agreement with the judge, we find that in the context of the ongoing dialogue among employees about tax withholding, Sanzone's comment effectively endorsed LaFrance's complaint that she owed money on her taxes due to a tax-withholding error on the Respondent's part. While Spinella's “like” is more ambiguous, we treat it for purposes of our analysis as expressing agreement with LaFrance's original complaint.¹⁸

¹⁸ The judge found that Spinella's “Like” referred to the “entire topic as it existed at the time”—i.e., up to and including LaFrance's comment: “It's all Ralph's fault. He didn't do the paperwork right. I'm calling the labor board to look into it bc he still owes me about 2000 in paychecks.” We disagree with the judge's interpretation of what it means for an individual to “Like” an individual's status update. We interpret Spinella's “Like” solely as an expression of approval of the

We reject the Respondent's contention that Sanzone or Spinella can be held responsible for any of the other comments posted in this exchange. Neither Sanzone nor Spinella accused the Respondent of pocketing employees' money or endorsed any comment by LaFrance to that effect. Assuming, arguendo, that such an accusation would have been unprotected, neither Sanzone nor Spinella would have lost the protection of the Act merely by participating in an otherwise protected discussion in which other persons made unprotected statements. See *Jefferson Standard*, 94 NLRB 1507, 1513 fn. 21 (1951), *affd. sub nom. NLRB v. Electrical Workers Local 1229 (Jefferson Standard)*, 346 U.S. 464 (1953); see also *Crowne Plaza LaGuardia*, 357 NLRB No. 95, slip op. at 4 fn. 11 (2011).

The comments at issue here are qualitatively different from the disparaging communications that lost protection in the *Jefferson Standard* case. First, the Facebook discussion here clearly disclosed the existence of an ongoing labor dispute concerning the Respondent's tax-withholding practices. Second, the evidence does not establish that the discussion in general, or Sanzone's and Spinella's participation in particular, was directed to the general public. The comments at issue were posted on an individual's personal page rather than, for example, a company page providing information about its products or services. Although the record does not establish the privacy settings of LaFrance's page, or of individuals other than Sanzone who commented in the discussion at issue, we find that such discussions are clearly more comparable to a conversation that could potentially be overheard by a patron or other third party than the communications at issue in *Jefferson Standard*, which were clearly directed at the public.

In any event, we find that Spinella's and Sanzone's comments were not “so disloyal . . . as to lose the Act's protection” under *Jefferson Standard* and its progeny. *MasTec*, 357 NLRB No. 17, slip op. at 5. The comments at issue did not even mention the Respondent's products or services, much less disparage them. Where, as here, the purpose of employee communications is to seek and provide mutual support looking toward group action to encourage the employer to address problems in terms or conditions of employment, not to disparage its product or services or undermine its reputation, the communications are protected. See *Valley Hospital*, 351 NLRB at 1252 fn. 7, and cases cited therein.

initial status update. Had Spinella wished to express approval of any of the additional comments emanating from the initial status update, he could have “liked” them individually.

The comments at issue likewise were not defamatory. Under the standard set forth in *Linn* and its progeny, the Respondent has the burden to establish that the comments were maliciously untrue, i.e., were made with knowledge of their falsity or with reckless disregard for their truth or falsity. E.g., *Springfield Library & Museum*, 238 NLRB 1673, 1673 (1979). The Respondent has failed to meet this burden; there is no basis for finding that the employees' claims that their withholding was insufficient to cover their tax liability, or that this shortfall was due to an error on the Respondent's part, were maliciously untrue.¹⁹ And Sanzone's characterization of DelBuono as an "asshole" in connection with the asserted tax-withholding errors cannot reasonably be read as a statement of fact; rather, Sanzone was merely (profanely) voicing a negative personal opinion of DelBuono. Accordingly, we find that these statements also did not lose protection under *Linn*. See *El San Juan Hotel*, 289 NLRB 1453, 1455 (1988) (leaflet's "references to the trustee as a 'Dictator' and as 'Robin Hood' [were] obvious rhetorical hyperbole"); *NLRB v. Container Corp. of America*, 649 F.2d 1213, 1214, 1215–1216 (6th Cir. 1981) (newsletter criticizing company's grievance process and calling the general manager a "slave driver" was protected rhetoric), enfg. in relevant part 244 NLRB 318 (1979).

3.

Having found that the Facebook activity at issue constituted protected concerted activity, and that conduct did not lose the protection of the Act, we must now decide whether the Respondent violated the Act by discharging Sanzone and Spinella. For the reasons set forth in the judge's decision, we adopt the judge's finding that the discharges of Sanzone and Spinella violated Section 8(a)(1) under *Wright Line*, 251 NLRB at 1083.²⁰

¹⁹ As noted above, Sanzone admitted at the hearing that she had no reason to believe that her withholding had been improperly calculated. But this admission does not establish that her statement, "I owe too," was untrue, let alone maliciously so. Sanzone and Spinella may have tacitly endorsed LaFrance's claim that the Respondent had erred in its tax withholding, but they did not repeat it. In any case, as the Board has noted, the fact that a statement may ultimately prove inaccurate does not in itself remove the statement from the protections of the Act when it is relayed by others. See *Valley Hospital*, 351 NLRB at 1253.

²⁰ We agree with the Respondent that the *Burnup & Sims* framework is not applicable here. Purporting to apply *Burnup & Sims*, the judge found that the discharges violated Sec. 8(a)(1), notwithstanding that the Respondent may have mistakenly believed, in good faith, that Sanzone's and Spinella's Facebook posts were unprotected. But *Burnup & Sims* applies in cases involving mistakes of fact, not mistakes of law. Under *Burnup & Sims*, an employer violates Sec. 8(a)(1) by disciplining or discharging an employee based on a good-faith belief that the employee engaged in misconduct during otherwise protected activity, if the General Counsel shows that the employee was not, in

II.

The judge dismissed the allegation that the Respondent's maintenance of its Internet/Blogging policy violated the Act.²¹ Because we find that employees would reasonably construe the policy to prohibit the type of protected Facebook posts that led to the unlawful discharges, we reverse.

The Respondent maintains the following work rule as part of its Internet/Blogging policy in its employee handbook:

The Company supports the free exchange of information and supports camaraderie among its employees. However, when internet blogging, chat room discussions, e-mail, text messages, or other forms of communication extend to employees revealing confidential and proprietary information about the Company, or engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment. Please keep in mind that if you communicate regarding any aspect of the Company, you must include a disclaimer that the views you share are yours, and not necessarily the views of the Company. In the event state or federal law precludes this policy, then it is of no force or effect.

A rule violates Section 8(a)(1) if it would reasonably tend to chill employees in the exercise of their Section 7 rights.²² If the rule explicitly restricts activities protected by Section 7, it is unlawful.²³ If it does not, "the violation is dependent upon a showing of one of the following: (1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights." *Lutheran Heritage Village*, 343 NLRB at 647. In analyzing work rules, the Board "must refrain from reading particular phrases in isolation, and . . . must not presume improper interference with employee rights." *Id.* at 646.

fact, guilty of that misconduct. "Otherwise," the Supreme Court explained, "the protected activity would lose some of its immunity, since the example of employees who are discharged on false charges would or might have a deterrent effect on other employees." 379 U.S. at 23. Plainly, this is not a "mistake of fact" case, and *Burnup & Sims* does not apply.

²¹ The General Counsel does not contend that the Respondent expressly relied on this policy in discharging Sanzone or Spinella or in undertaking any disciplinary action.

²² *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), enfd. 203 F.3d 52 (D.C. Cir. 1999).

²³ *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 646 (2004).

No party disputes the judge's finding that the Internet/Blogging policy does not explicitly restrict protected activity and was neither promulgated in response to, nor applied to restrict, protected activity. Accordingly, the inquiry here is whether the first prong of the *Lutheran Heritage* test is met. The judge found that the first prong was not met; in her view, employees would reasonably construe the Internet/Blogging policy's prohibition of "inappropriate discussions about the company, management, and/or coworkers" on social media as going no further than similar rules found lawful by the Board. On exceptions, the General Counsel contends that the prohibition on "inappropriate discussions" is overly broad and not comparable to restrictions on inappropriate conduct that the Board has found lawful, and that employees would interpret the rule in light of the unlawful discharges.

We find merit in the General Counsel's exception. An employer rule is unlawfully overbroad when employees would reasonably interpret it to encompass protected activities.²⁴ Here, we believe that employees would reasonably interpret the Respondent's rule as proscribing any discussions about their terms and conditions of employment deemed "inappropriate" by the Respondent. The rule contains only one other prohibition—against revealing confidential information—and provides no illustrative examples to employees of what the Respondent considers to be inappropriate. Under these circumstances, we find the term "inappropriate" to be "sufficiently imprecise" that employees would reasonably understand it to encompass "discussions and interactions protected by Section 7." *First Transit, Inc.*, 360 NLRB

No. 72, slip op. at 3 (quoting *2 Sisters Food Group*, 357 NLRB No. 168, slip op. at 2 (2011)).²⁵

Furthermore, by unlawfully discharging Sanzone and Spinella for participating in a Facebook discussion about the Respondent and its owners, the Respondent provided employees with an authoritative indication of the scope of its prohibition against inappropriate discussions and that they should construe its rule against inappropriate discussions to include such protected activity. See *The Roomstore*, 357 NLRB No. 143, slip op. at 1 fn. 3 (2011) (employees would reasonably construe rule prohibiting "[a]ny type of negative energy or attitudes" to include protected activity given employer's repeated warnings not to talk negatively about the employer's pay practices). Although the Respondent's Internet/Blogging policy contains a general savings clause stating that the policy "is of no force or effect" if "state or federal law precludes [it]," the two unlawful discharges served as an indication to employees that the clause did not shield Sanzone's and Spinella's protected activity. Faced with these discharges, employees therefore would reasonably construe the Internet/Blogging policy to prohibit Section 7 activity such as the Facebook discussion of tax withholding issues involved in this case.

Contrary to our dissenting colleague, we are not "cobbling together" two prongs of *Lutheran Heritage* to find the violation.²⁶ The test under the first prong of *Lutheran Heritage* is whether employees would reasonably construe the policy to prohibit their Section 7 activities. We do not believe that we will cause employers greater uncertainty in drafting rules by applying the first prong

²⁴ See, e.g., *First Transit, Inc.*, 360 NLRB No. 72, slip op. at 2–3 (2014) (finding rule prohibiting "[d]iscourteous or inappropriate attitude or behavior to passengers, other employees, or members of the public" unlawfully overbroad); *Hill & Dales General Hospital*, 360 NLRB No. 70, slip op. at 1–2 (2014) (finding unlawfully overbroad rules requiring employees to "represent [the employer] in the community in a positive and professional manner" and prohibiting "negative comments" and "negativity"); *Lafayette Park Hotel*, 326 NLRB 824, 828 (1998) (finding unlawfully overbroad rule prohibiting "false, vicious, profane or malicious statements toward or concerning [the employer] or any of its employees"). The Board's approach in this area has received judicial approval. See, e.g., *Cintas Corp. v. NLRB*, 482 F.3d 463, 469–470 (D.C. Cir. 2007) (approving the Board's finding that rule requiring employees to maintain "confidentiality of any information concerning the company, its business plans, its partners, new business efforts, customers, accounting and financial matters" was unlawfully overbroad), enfg. 344 NLRB 943 (2005); *Brockton Hospital v. NLRB*, 294 F.3d 100, 106 (D.C. Cir. 2002) (approving the Board's finding that rule prohibiting discussions of "[i]nformation concerning patients, associates, or hospital operations . . . except strictly in connection with hospital business" was unlawfully overbroad), enfg. 333 NLRB 1367 (2001).

²⁵ The "patent ambiguity" in the phrase "inappropriate discussions" distinguishes the Respondent's rule from the conduct rules found lawful in *Lutheran Heritage* "that were more clearly directed at unprotected conduct." *2 Sisters Food Group*, supra, slip op. at 2 (distinguishing the conduct rules found lawful in *Lutheran Heritage* from a rule prohibiting the "inability or unwillingness to work harmoniously with other employees" because of the "patent ambiguity" in the term "work harmoniously"). We also find distinguishable the cases relied on by our dissenting colleague and the judge where the Board found lawful rules that addressed conduct rather than merely addressing statements or that addressed the use of abusive, threatening, or slanderous statements.

²⁶ In *Albertson's, Inc.*, cited by our colleague, the Board rejected the analysis of the judge, who found three rules—each of which was lawful in isolation—unlawful when "informed by the context of the Respondent's actions at relevant times," including the maintenance of other overly restrictive rules regarding union buttons, solicitation, and distribution. 351 NLRB 254, 378 (2007). The Board stated bluntly that "[t]he judge also erred by lumping the three rules together in his analysis." Id. at 258. Moreover, the Board found that the individual rules could not be found unlawful by "bootstrapping them to other unrelated work rule violations" or analyzing them in the "'broader context' of unrelated unfair labor practices involving other rules." Id. at 258–259. We have done nothing of the sort here. The one and only rule we have considered is the Respondent's Internet/Blogging policy.

of *Lutheran Heritage* to the facts of this case. Our conclusion that the Internet/Blogging policy is unlawful is in accord with the many Board decisions that have found a rule unlawful if employees would reasonably interpret it to prohibit protected activities. Based on the Respondent's unlawful actions, we find that they would.²⁷ Accordingly, we find that the Respondent's maintenance of this rule violates Section 8(a)(1) of the Act.

AMENDED CONCLUSIONS OF LAW

Substitute the following for Conclusion of Law 8 in the judge's decision.

"8. The Respondent violated Section 8(a)(1) of the Act by maintaining the Internet/Blogging policy in its employee handbook."

ORDER

The National Labor Relations Board orders that the Respondent, Three D, LLC d/b/a Triple Play Sports Bar and Grille, Watertown, Connecticut, its officers, agents, successors, and assigns, shall

1. Cease and desist from

(a) Maintaining an Internet/Blogging policy that prohibits employees from engaging in "inappropriate discussions about the company, management, and/or co-workers."

(b) Discharging or otherwise discriminating against employees because they engage in protected concerted activities.

(c) Threatening employees with legal action in retaliation for their protected concerted activities.

(d) Informing employees that they are being discharged because they engaged in protected concerted activities.

²⁷ We disagree with our dissenting colleague's reading of the policy as providing that only an "inappropriate discussion" that violates the law would subject an employee to discipline. We find that reading inconsistent with the plain language of the policy. The policy states that "when . . . communication extend[s] to . . . inappropriate discussions . . . , the employee *may* be violating the law and *is* subject to disciplinary action, up to and including termination." (Emphasis added.) Thus, by the express terms of the policy, while only some "inappropriate discussions" may be unlawful, *all* "inappropriate discussions" subject the employee to discipline, including discharge. We believe that employees would reasonably read this language as informing them that inappropriate discussions subject them to disciplinary action regardless whether the discussion violates the law. Moreover, we recognize that employees could conceivably engage in "inappropriate discussions" that violate the law and, appropriately, result in discipline. However, the question before us is whether the Respondent's employees would reasonably conclude that the Respondent would consider their protected discussions on the Internet as "inappropriate," and grounds for discipline under the policy, because of the Respondent's discharge of Sanzone and Spinella for their protected activities in a Facebook discussion.

(e) Threatening employees with discharge in retaliation for their protected concerted activities.

(f) Coercively interrogating employees about their protected concerted activities.

(g) In any like or related manner interfering with, restraining, or coercing employees in the exercise of the rights guaranteed them by Section 7 of the Act.

2. Take the following affirmative action necessary to effectuate the policies of the Act.

(a) Revise or rescind the Internet/Blogging policy in the employee handbook that prohibits employees from engaging in "inappropriate discussions about the company, management, and/or co-workers."

(b) Furnish all current employees with inserts for the current employee handbook that (1) advise that the unlawful Internet/Blogging policy has been rescinded, or (2) provide the language of a lawful policy; or publish and distribute to all current employees a revised employee handbook that (1) does not contain the unlawful policy, or (2) provides the language of a lawful policy.

(c) Within 14 days from the date of this Order, offer Jillian Sanzone and Vincent Spinella full reinstatement to their former jobs or, if those jobs no longer exist, to substantially equivalent positions, without prejudice to their seniority or to any other rights or privileges previously enjoyed.

(d) Make Jillian Sanzone and Vincent Spinella whole for any loss of earnings and other benefits suffered as a result of the discrimination against them, in the manner set forth in the remedy section of the judge's decision as amended in this decision.

(e) Compensate Jillian Sanzone and Vincent Spinella for the adverse tax consequences, if any, of receiving lump-sum backpay awards, and file a report with the Social Security Administration allocating the backpay awards to the appropriate calendar quarters for each employee.

(f) Within 14 days from the date of this Order, remove from its files any reference to the unlawful discharges of Jillian Sanzone and Vincent Spinella, and within 3 days thereafter, notify Sanzone and Spinella in writing that this has been done and that the discharges will not be used against them in any way.

(g) Preserve and, within 14 days of a request, or such additional time as the Regional Director may allow for good cause shown, provide at a reasonable place designated by the Board or its agents, all payroll records, social security payment records, timecards, personnel records and reports, and all other records, including an electronic copy of such records if stored in electronic form, necessary to analyze the amount of backpay due under the terms of this Order.

TRIPLE PLAY SPORTS BAR & GRILLE

(h) Within 14 days after service by the Region, post at its facility in Watertown, Connecticut, copies of the attached notice marked "Appendix."²⁸ Copies of the notice, on forms provided by the Regional Director for Region 34, after being signed by Respondent's authorized representative, shall be posted by the Respondent and maintained for 60 consecutive days in conspicuous places, including all places where notices to employees are customarily posted. In addition to physical posting of paper notices, notices shall be distributed electronically, such as by email, posting on an intranet or an internet site and/or other electronic means, if the Respondent customarily communicates with its employees by such means. Reasonable steps shall be taken by the Respondent to ensure that the notices are not altered, defaced, or covered by any other material. If the Respondent has gone out of business or closed the facility involved in these proceedings, the Respondent shall duplicate and mail, at its own expense, a copy of the notice to all current employees and former employees employed by the Respondent at any time since August 16, 2010.

(i) Within 21 days after service by the Region, file with the Regional Director for Region 34 a sworn certification of a responsible official on a form provided by the Region attesting to the steps that the Respondent has taken to comply.

Dated, Washington, D.C. August 22, 2014

Kent Y. Hirozawa, Member

Nancy Schiffer, Member

(SEAL) NATIONAL LABOR RELATIONS BOARD
MEMBER MISCIMARRA, dissenting in part.

I join my colleagues in finding that the Respondent unlawfully discharged employees Jillian Sanzone and Vincent Spinella for their protected, concerted participation in a Facebook discussion, and I agree with the analysis the majority opinion applies in reaching those findings.¹

²⁸ If this Order is enforced by a judgment of a United States court of appeals, the words in the notice reading "Posted by Order of the National Labor Relations Board" shall read "Posted Pursuant to a Judgment of the United States Court of Appeals Enforcing an Order of the National Labor Relations Board."

¹ When communications by employees with third parties or the general public are at issue, the Board generally has applied the standards set forth in *NLRB v. Electrical Workers Local 1229 (Jefferson Stand-*

I also agree that the Respondent violated the Act by threatening employees with discharge, by interrogating employees about their Facebook activity, and by threatening Spinella with legal action for engaging in that activity.² As discussed below, however, I disagree with their finding that the Respondent's Internet/blogging policy violated the Act.

The Respondent maintained a facially lawful Internet/Blogging policy to prevent disclosure of its proprietary or confidential information by its employees, to help ensure that unauthorized statements by employees would not be attributed to the Respondent, and to warn employees about "inappropriate discussions" that could be unlawful and subject them to discipline. The policy states as follows:

The Company supports the free exchange of information and supports camaraderie among its employees. However, when internet blogging, chat room discussions, e-mail, text messages, or other forms of communication extend to employees revealing confidential and proprietary information about the Company, or en-

ard), 346 U.S. 464 (1953), and *Linn v. Plant Guards Local 114*, 383 U.S. 53 (1966), and not *Atlantic Steel Co.*, 245 NLRB 814 (1979). When such communications take place in the presence of customers in a retail establishment and involve conduct that seriously disrupts the employer's business and interferes with its ability to serve its patrons in an atmosphere free of interruption and unwanted intrusion, the applicable standard is set forth in *Restaurant Horikawa*, 260 NLRB 197 (1982). See also *Starbucks Coffee Co.*, 360 NLRB No. 134, slip op. at 7 (2014) (Member Miscimarra, concurring). In addition, I believe that social-media communications may lose the Act's protection where, for example, they are "so egregious as to take [them] outside the protection of the Act, or of such character as to render the employee unfit for further service." *Neff-Perkins Co.*, 315 NLRB 1229, 1229 fn. 2, 1233-1234 (1994) (quoting *Consumers Power Co.*, 282 NLRB 130, 132 (1986)). Here, Sanzone and Spinella did not lose the Act's protection under any standard.

² Unlike my colleagues, I do not find that the Respondent separately violated Sec. 8(a)(1) of the Act by *telling* Sanzone and Spinella that their protected Facebook activity was the reason they were being discharged. Merely advising employees of the reason for their discharge is "part of the res gestae of the unlawful termination, and is subsumed by that violation." *Benesight, Inc.*, 337 NLRB 282, 285 (2001) (Chairman Hurtgen, dissenting in part).

My colleagues find it unnecessary to pass on the judge's finding that the Respondent also unlawfully threatened Sanzone with legal action. I would dismiss this allegation. The Respondent informed Sanzone that it would commence an action for defamation against her in a letter from its counsel requesting that she retract her allegedly defamatory statements. That letter was sent to Sanzone pursuant to a provision of Connecticut law cited in the letter requiring such a request prior to the institution of an action for defamation. Because the letter was procedurally prerequisite to filing a lawsuit, I would not find it unlawful absent a showing by the General Counsel that a defamation lawsuit against Sanzone would have violated Sec. 8(a)(1). See *BE & K Construction Co. v. NLRB*, 536 U.S. 516 (2002). No such showing was attempted here.

gaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment. Please keep in mind that if you communicate regarding any aspect of the Company, you must include a disclaimer that the views you share are yours, and not necessarily the views of the Company. In the event state or federal law precludes this policy, then it is of no force or effect.

The policy does not expressly or implicitly restrict Section 7 activity, and it was not promulgated in response to such activity. Neither has it been applied to restrict protected activity: the Respondent did not apply or in any way refer to the policy when it discharged Sanzone and Spinella. Nor is there any language in the policy that employees would reasonably construe to prohibit Section 7 activity. The Policy is legitimately aimed to prevent the revelation of proprietary information and statements about the company, its management, and its employees that may be unlawful.

The judge correctly dismissed the allegation, under the first prong of *Lutheran Heritage Village-Livonia*, 343 NLRB 646, 646–647 (2004), that employees would reasonably construe the language warning them against “inappropriate discussions about the company, management, and/or co-workers” to prohibit Section 7 activity.³ She observed that the language the General Counsel challenged is similar to restrictions on speech or conduct (including speech) in other work rules that the Board has found lawful.⁴

³ I do not agree with the current Board standard regarding alleged overly broad rules and policies, which is set forth as the first prong of *Lutheran Heritage* (finding rules and policies unlawful, even if they do not explicitly restrict protected activity and are not applied against or promulgated in response to such activity, where “employees would reasonably construe the language to prohibit Section 7 activity”). I would reexamine this standard in an appropriate future case. I agree with the judge, however, that the policy here is lawful under the *Lutheran Heritage* standard. In fact, for the reasons set forth in the text, I believe the policy is phrased in general commonsense terms that preclude it from reasonably being considered unlawful under any standard.

⁴ See, e.g., *Tradesmen International*, 338 NLRB 460, 462–463 (2002) (finding lawful rule prohibiting “verbal or other statements which are slanderous or detrimental to the company or any of the company’s employees”); *Ark Las Vegas Restaurant Corp.*, 335 NLRB 1284 fn. 2, 1291–1292 (2001) (finding lawful rules prohibiting “any conduct” that “reflects adversely on yourself, fellow associates, [or] the Company,” or “conducting oneself unprofessionally or unethically, with the potential of damaging the reputation or a department of the Company”), enf’d. in part 334 F.3d 99 (D.C. Cir. 2003); see also *Community Hospitals of Central California v. NLRB*, 335 F.3d 1079, 1088–1089 (D.C. Cir. 2003) (finding lawful rule prohibiting “insubordination . . . or other disrespectful conduct”), denying enf. in pertinent part to 335 NLRB 1318 (2001).

For several reasons, I do not agree with my colleagues’ theory that employees would reasonably understand the rule to encompass Section 7 activity on the basis that (i) it uses an “imprecise” word—“inappropriate”—without providing “illustrative examples,” and (ii) the Respondent discharged Spinella and Sanzone for their protected Facebook activity.

First, the Respondent neither cited nor applied its Internet/Blogging policy in discharging Spinella or Sanzone. It did not accuse them of revealing confidential or proprietary information or assert that they had engaged in “inappropriate conversations about the company.” Rather, it claimed their Facebook comments were disloyal and defamatory. Under these circumstances, there is no factual basis for the majority to conclude that the discharges provided employees with an “authoritative indication” of how the Internet/Blogging policy should be construed.

Second, this cobbling together prongs one and three of the *Lutheran Heritage Village* standard is contrary to the careful separation of those two theories of violation established in that case. Under prong one, the inquiry is whether the language of a rule, on its face, would reasonably be interpreted to prohibit Section 7 activity. Under prong three, the inquiry is whether a rule, *regardless* of its wording, has been applied to restrict the exercise of Section 7 rights. Following *The Roomstore*, 357 NLRB No. 143 (2011)—in my view, incorrectly decided in this regard—the majority continues down the path of this hybrid category of violation, under which a rule that is not unlawful on its face and has not been applied to restrict the exercise of Section 7 rights nevertheless is found unlawful based on a mixture of the rule’s language and the employer’s conduct.⁵ In so doing, the majority contributes to the uncertainty employers confront in seeking to square their rules with our *Lutheran Heritage* prong-one precedent, which, at this point, consists of so many distinctions, qualifications, and factual variations as to preclude any reasonable “certainty beforehand” for most parties “as to when [they] may proceed to reach

⁵ The Board rejected a similar analysis in *Albertson’s, Inc.*, 351 NLRB 254, 258–259 (2007). There, the judge improperly bootstrapped the employer’s unlawful application of one rule to restrict the exercise of Sec. 7 rights to find unlawful two other rules lawful in themselves. My colleagues distinguish *Albertson’s* as involving multiple rules while this case involves only one. However, the judge in *Albertson’s* went outside the plain language of the challenged rules and applied an analysis “informed by the context of the Respondent’s actions at relevant times, including the history of improper restriction of employees’ Section 7 rights.” *Id.* at 378. The Board properly rejected that approach, and my colleagues here embrace it.

decisions without fear of later evaluations labeling [their] conduct an unfair labor practice.”⁶

Third, I do not believe one can reasonably construct a theory that it constitutes unlawful restraint, coercion, or interference with protected concerted activities to advise employees, as set forth in the policy, that an employee “may be violating the law and is subject to disciplinary action” if their internet communications “extend to employees revealing *confidential and proprietary information about the Company*, or engaging in *inappropriate discussions* about the company, management, and/or co-workers” (emphasis added). Nobody can seriously disagree that the two listed infractions—disclosing “confidential and proprietary information” and “inappropriate discussions”—“may” violate one or more laws “and” be proper grounds for discipline. Although the reference to “inappropriate” discussions is potentially susceptible to different interpretations, there is no law against using an understandable catchall phrase as a general statement of policy, particularly in the circumstances presented here (where employees are advised such discussions “may” violate the law and make the offenders “subject to” discipline). It is also significant that the reference to possible legal violations and potential discipline is phrased in the conjunctive (the two concepts are connected by “and,” not “or”). Thus, the policy states, in effect, that “inappropriate discussions,” *if* they violate the law, may also “subject” the offending employees to discipline.⁷

Most people appreciate that “inappropriate” behavior may have consequences sufficiently serious as to violate the law and result in discipline. It does not per se violate Federal labor law to use a general phrase to describe the type of conduct that may do so.⁸ If it did, “just cause” provisions contained in most collective-bargaining

agreements that have been entered into since the Act’s adoption nearly 80 years ago would be invalid.⁹ However, “just cause” provisions have been called “an obvious illustration” of the fact that many provisions “must be expressed in general and flexible terms.”¹⁰ More generally, the Supreme Court has stated, in reference to collective-bargaining agreements, that there are “a myriad of cases which the draftsmen cannot wholly anticipate,” and “[t]here are too many people, too many problems, too many unforeseeable contingencies to make the words . . . the exclusive source of rights and duties.”¹¹ The policy at issue in the instant case makes reference to “inappropriate discussions” in the same manner, which precludes reasonably regarding this phrase as unlawful interference, restraint or coercion.¹²

Finally, the Board is finding that Sanzone’s and Spinella’s discharges were unlawful, and the policy’s disclaimer states that the policy “is of no force or effect” if State or Federal law precludes it. Thus, even if the discharges had some bearing on interpretations of the policy (notwithstanding the fact that the Respondent here never invoked or relied upon the policy in relation to the discharges), the policy on its face disclaims any application in circumstances that would be unlawful. Although a general disclaimer may not be sufficient to render valid language that explicitly runs afoul of the Act’s requirements, such a disclaimer reinforces that the policy is meant to be interpreted in a manner not contrary to appli-

⁶ *First National Maintenance Corp. v. NLRB*, 452 U.S. 666, 679 (1981).

⁷ Notwithstanding this phrasing, my colleagues believe that employees would read the policy as subjecting them to discipline for any discussion the Respondent deems inappropriate, “regardless whether the discussion violates the law.” In other words, in their view, the reference in the policy to communications that violate the law has no effect on how employees would read the policy; they would read it the same way with or without that language. This interpretation may be conceivable, but it is not reasonable. See *Lutheran Heritage Village*, 343 NLRB at 647 (rejecting an analytical approach that would “require the Board to find a violation whenever the rule could conceivably be read to cover Section 7 activity, even though that reading is unreasonable”).

⁸ To the contrary, as the Board observed in *Lutheran Heritage Village*, “[w]ork rules are necessarily general in nature We will not require employers to anticipate and catalogue in their work rules every instance in which [prohibited types of speech] might conceivably be protected by (or exempted from the protection of) Section 7.” 343 NLRB at 648. My colleagues’ apparent requirement that employers include “illustrative examples” of general terms to avoid violating the Act is difficult to square with that decision.

⁹ “Just cause” provisions—which state that employees are subject to discipline or discharge if there is “just cause”—have been ubiquitous in collective-bargaining agreements throughout the Act’s history. See, e.g., *Burgie Vinegar Co.*, 71 NLRB 829, 840 (1946) (“It is agreed that the right to discharge employees for just cause is a management prerogative.”); *Solutia, Inc.*, 357 NLRB No. 15, slip op. at 4 fn. 8 (2011) (contract reserves to the company the right to “discipline or discharge for just cause”), *enfd.* 699 F.3d 50 (1st Cir. 2012).

¹⁰ Archibald Cox, *Reflections Upon Labor Arbitration*, 72 Harv. L. Rev. 1482, 1491 (1959).

¹¹ *Steelworkers v. Warrior & Gulf Navigation Co.*, 363 U.S. 574, 578–579 (1960) (quoting Cox, *supra* fn. 38, 72 Harv. L. Rev. at 1498–1499).

¹² Although my colleagues cite D.C. Circuit decisions in which the court approved the Board’s analysis in cases involving overly broad confidentiality rules, those cases are distinguishable from the instant case, and that court has criticized Board decisions finding rules unlawful because, like here, they employed general language to prohibit serious misconduct. See *Adtranz ABB Daimler-Benz Transportation, N.A., Inc. v. NLRB*, 253 F.3d 19, 28 (D.C. Cir. 1991) (admonishing Board to not “pars[e] workplace rules too closely in a search for ambiguity that could limit protected activity”); *Community Hospitals of Central California v. NLRB*, *supra* at 1089 (“[T]o quote the Board itself in a more realistic moment, ‘any arguable ambiguity’ in the rule ‘arises only through parsing the language of the rule, viewing the phrase . . . in isolation, and attributing to the [employer] an intent to interfere with employee rights’” (quoting *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998))).

cable law. For this reason as well, I believe the policy is lawful, and the majority should not require the Respondent to rescind or revise it.

Dated, Washington, D.C. August 22, 2014

Philip A. Miscimarra, Member

NATIONAL LABOR RELATIONS BOARD

APPENDIX

NOTICE TO EMPLOYEES

POSTED BY ORDER OF THE

NATIONAL LABOR RELATIONS BOARD

An Agency of the United States Government

The National Labor Relations Board has found that we violated Federal labor law and has ordered us to post and obey this notice.

FEDERAL LAW GIVES YOU THE RIGHT TO

Form, join, or assist a union

Choose representatives to bargain with us on your behalf

Act together with other employees for your benefit and protection

Choose not to engage in any of these protected activities.

WE WILL NOT maintain an Internet/Blogging policy that prohibits employees from engaging in “inappropriate discussions about the company, management, and/or co-workers.”

WE WILL NOT discharge or otherwise discriminate against any of you for engaging in protected concerted activities.

WE WILL NOT threaten you with legal action in retaliation for your protected concerted activities.

WE WILL NOT inform you that you are being discharged because you engaged in protected concerted activities.

WE WILL NOT threaten you with discharge in retaliation for your protected concerted activities.

WE WILL NOT coercively question you about your protected concerted activities.

WE WILL NOT in any like or related manner interfere with, restrain, or coerce you in the exercise of the rights listed above.

WE WILL, within 14 days of the Board’s Order, revise or rescind the Internet/Blogging policy in the employee handbook that prohibits employees from engaging in “inappropriate discussions about the company, manage-

ment, and/or co-workers,” and WE WILL advise employees in writing that we have done so and that the unlawful rules will no longer be enforced.

WE WILL furnish you with inserts for the current employee handbook that (1) advise that the unlawful Internet/Blogging policy has been rescinded, or (2) provide the language of a lawful policy; or WE WILL publish and distribute to all current employees a revised employee handbook that (1) does not contain the unlawful policy, or (2) provides the language of a lawful policy.

WE WILL, within 14 days from the date of the Board’s Order, offer Jillian Sanzone and Vincent Spinella full reinstatement to their former jobs or, if those jobs no longer exist, to substantially equivalent positions, without prejudice to their seniority or any other rights or privileges previously enjoyed.

WE WILL make Jillian Sanzone and Vincent Spinella whole for any loss of earnings and other benefits resulting from their discharge, less any net interim earnings, plus interest.

WE WILL compensate Jillian Sanzone and Vincent Spinella for the adverse tax consequences, if any, of receiving lump-sum backpay awards, and WE WILL file a report with the Social Security Administration allocating the backpay awards to the appropriate calendar quarters for each of them.

WE WILL, within 14 days from the date of the Board’s Order, remove from our files any reference to the unlawful discharges of Jillian Sanzone and Vincent Spinella, and WE WILL, within 3 days thereafter, notify each of them in writing that this has been done and that the discharges will not be used against them in any way.

THREE D, LLC D/B/A TRIPLE PLAY SPORTS BAR AND GRILLE

The Board’s decision can be found at www.nlr.gov/case/34-CA-012915 or by using the QR code below. Alternatively, you can obtain a copy of the decision from the Executive Secretary, National Labor Relations Board, 1099 14th Street, N.W., Washington, D.C. 20570, or by calling (202) 273-1940.



TRIPLE PLAY SPORTS BAR & GRILLE

Claire Sellers, Esq. and Jennifer Dease, Esq., for the Acting General Counsel.

Melissa Scozzafava, Esq. (Yamin & Grant, LLC), for the Respondent.

DECISION

STATEMENT OF THE CASE

LAUREN ESPOSITO, Administrative Law Judge. Based on a charge filed on February 16, 2011, and amended on March 7 and April 5, 2011, by Jillian Sanzone, an individual (Sanzone), and upon a charge filed on February 24, 2011, and amended on April 8, 2011, by Vincent Spinella, an individual (Spinella), a consolidated complaint and notice of hearing issued on August 17, 2011. The complaint alleges that Three D, LLC d/b/a Triple Play Sports Bar and Grille (Triple Play or Respondent) violated Section 8(a)(1) of the National Labor Relations Act (the Act) by discharging Sanzone and Spinella on February 2 and 3, 2011, respectively, in retaliation for their protected concerted activities. The consolidated complaint also alleges that Respondent violated Section 8(a)(1) by coercively interrogating and threatening employees, informing them that they were discharged because of their protected concerted activities, threatening them with legal action in retaliation for their protected concerted activities, and maintaining an unlawful policy in its employee handbook. Respondent filed an answer denying the material allegations of the complaint. This case was tried before me on October 18, 2011, in New York, New York.

On the entire record, including my observation of the demeanor of the witnesses, and after considering the briefs filed by the Acting General Counsel (the General Counsel) and Respondent I make the following

FINDINGS OF FACT

I. JURISDICTION

Respondent is a Connecticut limited liability corporation with a place of business located in Watertown, Connecticut, where it operates a sports bar and restaurant. Respondent admits and I find that it is an employer engaged in commerce within the meaning of Section 2(2), (6), and (7) of the Act.

II. ALLEGED UNFAIR LABOR PRACTICES

A. Background

Respondent began its operations in December 2009. At all times material to the events at issue in this case, Ralph DelBuono and Thomas Daddona have owned Respondent's business. DelBuono and Daddona oversee the restaurant's day-to-day operations, including the supervision of employees. DelBuono is also responsible for Respondent's accounting. Respondent admits and I find that DelBuono and Daddona are supervisors within the meaning of Section 2(11) of the Act. Respondent also admits and I find that Lucio Dibona is an agent of Respondent within the meaning of Section 2(13) of the Act. Finally, Respondent admits and I find that its attorney, Joseph P. Yamin, was Respondent's agent within the meaning of Section 2(13) of the Act with respect to the actions he took on Respondent's behalf.

B. The Employment of Jillian Sanzone and Vincent Spinella, and their Alleged Protected Concerted Activity

Jillian Sanzone was hired by Respondent when its operations began in December 2009, and worked continuously until her discharge on February 2, 2011. Sanzone worked as a waitress on Monday evenings, and as a bartender on Wednesday evenings, Thursday during the day, Friday days and evenings, and Saturday evenings. She clocked in and out through Respondent's computer system, and received a paycheck every Friday. During her employment, Sanzone received two raises, one 4 or 5 months after her employment began, and the second around Thanks-giving 2010. She also received a cash Christmas bonus in 2010.

Vincent Spinella began working for Respondent as a cook in September 2010, and worked from Wednesday through Sunday, for at least 8 hours per shift. He clocked in by punching a timecard, and received a paycheck every week. Spinella also received a cash Christmas bonus in 2010, together with a restaurant gift certificate.

Sanzone and Spinella both have accounts on the website Facebook, as does Respondent. Sanzone and Spinella both testified that prior to February 1, 2011, they had written about their employment with Respondent on their Facebook accounts. Sanzone had suggested that others visit the restaurant during her bartending shifts. Spinella had listed the restaurant's special dishes of the day, and suggested that others visit to watch particular sporting events. Both testified that prior to February 1, 2011, they had never been told that they were not permitted to write about Respondent on their Facebook accounts.

In January 2011,¹ when Sanzone filed her tax returns for 2010, she discovered that she owed taxes to the State of Connecticut. Sanzone testified that the Wednesday night prior to her discharge, waitress Amanda Faroni approached her and asked whether she had filed her tax return for the previous year. Sanzone said that she had done so, and that she owed about \$200 in taxes to the State. Faroni said that she was required to pay additional taxes to the State as well. Waiter Anthony Cavallo then approached them, and said that he was getting his taxes done soon, and hoped that he did not owe anything. Daddona testified that he was aware that employees were concerned with this issue, and that as a result he and DelBuono had arranged for a staff meeting with Respondent's accountant and payroll company. This meeting was to take place a week or two after Sanzone and Spinella were discharged.

On February 1, Sanzone read and commented on a posting about Respondent on the Facebook account of a former employee named Jamie LaFrance. LaFrance had worked with Sanzone at the bar, and left her employment with Respondent in November 2010. Sanzone was "friends" with LaFrance on Facebook, meaning that she was permitted by LaFrance to write on the "wall" of LaFrance's Facebook account. On January 31, LaFrance posted a comment on her "wall" stating, "Maybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork

¹ All subsequent dates are in 2011, unless otherwise indicated.

correctly!!! Now I OWE money Wtf!!!!” (Emphasis in original). The postings on LaFrance’s Facebook “wall” continued as follows:

KEN DESANTIS (customer): You owe them money . . . that’s f—ked up.

DANIELLE MARIE PARENT (employee): I F—KING OWE MONEY TOO!

LAFRANCE: The state. Not Triple Play. I would never give that place a penny of my money. Ralph f—ked up the paperwork . . . as per usual.

DESANTIS: Yeah I really don’t go to that place anymore.

LAFRANCE: It’s all Ralph’s fault. He didn’t do the paperwork right. I’m calling the labor board to look into it because he still owes me about 2000 in paychecks.

LAFRANCE: We shouldn’t have to pay it. It’s every employee there that it’s happening to.

DESANTIS: You better get that money . . . that’s bullshit if that’s the case I’m sure he did it to other people too.

PARENT: Let me know what the board says because I owe \$323 and I’ve never owed.

LAFRANCE: I’m already getting my 2000 after writing to the labor board and them investigating but now I find out he f—ked up my taxes and I owe the state a bunch. Grrr.

PARENT: I mentioned it to him and he said that we should want to owe.

LAFRANCE: Hahahaha he’s such a shady little man. He probably pocketed it all from all our paychecks. I’ve never owed a penny in my life till I worked for him. That goodness I got outta there.

SANZONE: I owe too. Such an asshole.

PARENT: Yeah me neither, I told him we will be discussing it at the meeting.

SARAH BAUMBACH (employee): I have never had to owe money at any jobs . . . I hope I won’t have to at TP . . . probably will have to seeing as everyone else does!

LAFRANCE: Well discuss good because I won’t be there to hear it. And let me know what his excuse is ☺.

JONATHAN FEELEY (customer): And they’re way too expensive.²

Spinella clicked “Like” under LaFrance’s initial comment, and the text “Vincent VinnyCenz Spinella and Chelsea Molloy like this” appears beneath it. Spinella testified that at the time he clicked “Like,” the last comment on the wall was LaFrance’s statement, “It’s all Ralph’s fault. He didn’t do the paperwork right. I’m calling the labor board to look into it because he still owes me about 2000 in paychecks.”

Daddona testified that he learned of the discussion on LaFrance’s Facebook account from his sister, Jobie Daddona, who also works at the restaurant. He and DelBuono then

logged onto Facebook,³ and DelBuono printed out a hard copy of the comments from LaFrance’s account.

C. The Discharge of Jillian Sanzone

Sanzone testified that when she arrived for work on February 2, Daddona spoke to her as she entered the building. Daddona told her that the Company had to make some changes, and that they had to let her go. Sanzone treated the statement as a joke, and Daddona reiterated that they had to fire her. Sanzone asked why, and Daddona said that she was not loyal enough to be working with Respondent because of her comment on Facebook. Daddona said that he had learned about Sanzone’s Facebook comment from customers. Sanzone protested that she worked hard, worked holidays, and did various favors for DelBuono and Daddona, all of which demonstrated her loyalty to the Company. Daddona responded that Sanzone was not loyal because of her Facebook comment. Sanzone then asked for a “pink slip” and her last paycheck. Daddona did not respond, and Sanzone left.

Daddona testified that Sanzone was discharged because her Facebook comment indicated that she was disloyal, and based on several incidents where at the end of her shift her cash register held more money than could be accounted for by totaling individual receipts.

D. The Discharge of Vincent Spinella

Spinella testified that when he arrived at work on February 3, Daddona asked him to come to the office downstairs. DelBuono was in the office, and the Facebook comments on LaFrance’s account were displayed on the screen of the office computer. DelBuono asked Spinella if there was a problem with him and Daddona, or with the Company, and Spinella replied that he had no such problems. DelBuono said that LaFrance’s Facebook wall indicated the opposite. DelBuono and Daddona proceeded to ask Spinella about the various comments, and about the significance of the “Like” option that Spinella had chosen. DelBuono asked Spinella whether he had written anything negative about DelBuono and Daddona, and Spinella said that he hadn’t written anything; he had only clicked the “Like” option. DelBuono also asked Spinella who Chelsea Molloy was, and Spinella explained that he did not know. DelBuono then told Daddona that the “Like” option meant that Spinella stood behind the other commenters, and asked Daddona whether Spinella had their best interests in mind given that he clicked the “Like” option. Daddona responded that this demonstrated that Spinella did not have their best interests in mind. DelBuono then said that his attorney had informed him that he should discharge anyone involved in the Facebook conversation for defamation. Spinella stated that the restaurant was DelBuono and Daddona’s business, and that if they believed that his clicking the “Like” option was grounds for discharge, he understood that they felt they had to do so. DelBuono told Spinella that it was time for him to go home for good, and Spinella then left. As Spinella was leaving,

² GC Exh. 2. Participants have been identified, and minor spelling, grammatical, and punctuation errors corrected, in the interests of clarity. Parent and Baumbach were employed by Respondent as of February 2011, but have since left Respondent’s employ.

³ Daddona testified that Respondent also has its own Facebook account.

DelBuono told him that he would be hearing from Respondent's attorneys.

Daddona testified that Spinella was discharged for poor work performance, including excessive cell phone use, conversing with the waitresses, and cigarette breaks, and failure to perform his work in an expedient manner. Daddona testified that Spinella's having chosen the "Like" option on LaFrance's Facebook account was not a factor in the decision to discharge him, and was not discussed during the conversation terminating his employment. Daddona testified that when he and DelBuono met with Spinella, they asked whether he was happy working for them, and asked him to provide a reason why he should remain employed, given his work performance. Daddona testified that when Spinella did not respond, he and DelBuono felt that Spinella was not interested in continuing his employment.

DelBuono also testified regarding Spinella's discharge meeting. DelBuono said that he and Daddona decided to meet with Spinella because Spinella's "Facebook comment raised a red flag," and made it apparent that he was unhappy. During the meeting, DelBuono told Spinella that he was obviously not happy, and then "questioned him," asking him, "if he liked those defamatory and derogatory statements so much well why is he still working for us?" DelBuono told Spinella that because he "liked the disparaging and defamatory comments," it was "apparent" that Spinella wanted to work somewhere else. He asked Spinella to provide "one valid reason why you want to continue working for us," and Spinella made no response and left.

Spinella testified that later on the day of his discharge he called Daddona to inquire about his final paycheck. He left a message for Daddona, which DelBuono returned. After they arranged for Spinella to receive his paycheck, Spinella asked DelBuono whether he would need any additional paperwork to file for unemployment, and DelBuono stated that Respondent's attorneys would not permit him to receive unemployment benefits.

E. Respondent's Threat to Institute an Action for Defamation Against Sanzone

On February 4, Respondent's attorney, Joseph P. Yamin of Yamin & Grant, LLC, wrote to Sanzone, stating as follows:

We represent Three D, LLC d/b/a Triple Play Sports Bar and its principals, Thomas Daddona, Ralph Delbuono, and Lucio Dibona. Pursuant to Connecticut General Statute § 52-237 (a copy is attached), this letter is a formal request for you to retract, in as public a manner as they were made, the defamatory statements regarding Triple Play and its principals published to the general public on Facebook. To refresh your recollection of those statements, attached are the excerpts from the Facebook website. Provide us with written confirmation that you have retracted your defamatory statements. If such statements are not retracted within thirty (30) days, we will be forced to commence an action for defamation against you.

Because users of Facebook are unable to delete the comments they post on another user's account, Sanzone asked

LaFrance to delete the comment she had made on LaFrance's "wall" regarding owing money on her taxes. LaFrance deleted Sanzone's comment.⁴ LaFrance had been sent a letter identical to Yamin's letter to Sanzone, and LaFrance had posted a retraction. On February 26, Sanzone sent Yamin a letter stating that her comment on LaFrance's Facebook page had been erased, and that she had filed a charge with the National Labor Relations Board. On March 1, Yamin responded that "[a] retraction requires that you post a formal statement that the defamatory statements were not true. Provide us with written confirmation that you have retracted your defamatory statements." Sanzone did not respond, and did not post any other statement or communicate with Yamin again.

The evidence establishes that no lawsuit was ever filed against Sanzone, Spinella, or LaFrance.

F. Respondent's Internet/Blogging Policy

Respondent maintains a handbook containing employee guidelines, which, according to Delbuono, was discussed with Respondent's initial employees when the restaurant began its operations in December 2009. Delbuono testified that at employee orientation the handbook was passed around among the employees, and that he told the employees that they could request their own copy. As discussed above, Sanzone was one of Respondent's initial employees.

The "Internet/Blogging Policy" contained in Respondent's employee guidelines states as follows:

The Company supports the free exchange of information and supports camaraderie among its employees. However, when internet blogging, chat room discussions, e-mail, text messages, or other forms of communication extend to employees revealing confidential and proprietary information about the Company, or engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment. Please keep in mind that if you communicate regarding any aspect of the Company, you must include a disclaimer that the views you share are yours, and not necessarily the views of the Company. In the event state or federal law precludes this policy, then it is of no force or effect.

III. ANALYSIS AND CONCLUSIONS

A. The Discharges of Jillian Sanzone and Vincent Spinella

1. Summary of the Parties' contentions

The General Counsel contends that Respondent's decision to discharge Sanzone and Spinella was based entirely on their having participated in the conversation on LaFrance's Facebook account. The General Counsel argues as a result that the discharges must be considered pursuant to the analysis articulated by the Supreme Court in *NLRB v. Burnup & Sims*, 379 U.S. 21 (1964). Under *Burnup & Sims*, an employer violates Section 8(a)(1) when the discharged employee was engaged in

⁴ Spinella testified that after Sanzone was discharged he rescinded his selection of the "Like" option on LaFrance's Facebook account.

protected activity at the time of their purported misconduct, the employer knew of the protected activity, the basis for the discharge was the employee's alleged misconduct in the course of their protected activity, and the employee was not actually guilty of the misconduct. The General Counsel thus argues that Sanzone and Spinella's participation in the Facebook conversation was protected concerted activity, that Respondent was aware of their participation, that Respondent discharged them for the comments constituting alleged misconduct, and that Sanzone and Spinella did not in fact commit misconduct causing them to lose the Act's protection. Applying the Board's analysis articulated in *Atlantic Steel Co.*, 245 NLRB 814, 816–817 (1979), the General Counsel argues that given the location and subject matter of the Facebook discussion, the nature of the “outburst,” and the extent to which the outburst was provoked by Respondent's conduct, Sanzone and Spinella's comments on LaFrance's Facebook account remained protected activity. General Counsel also argues that Sanzone and Spinella's comments did not constitute disparaging and disloyal statements unprotected under *NLRB v. Electrical Workers Local 1229 (Jefferson Standard)*, 346 U.S. 464 (1953), and its progeny. Finally, the General Counsel contends that, to the extent that the *Wright Line* analysis may be applicable, it has established a prima facie case and Respondent has failed to establish by a preponderance of the credible evidence that it in fact discharged Sanzone and Spinella for other, legitimate, reasons.

Respondent contends in its posthearing brief that Sanzone was discharged for “disloyalty,” consisting of her “disparaging attack” on DelBuono during the Facebook discussion, and repeated cash register inaccuracies. Respondent argues that Sanzone's comment on LaFrance's Facebook account was unprotected under *Jefferson Standard*. Respondent contends that Spinella was discharged for poor work performance, and not for any participation in the Facebook discussion. However, Respondent contends that even if Spinella had been discharged for his participation in the Facebook conversation, his having selected the “Like” option would constitute unprotected disloyalty and disparagement under *Jefferson Standard*. Respondent further contends that Sanzone and Spinella's comments were defamatory and unprotected under *Linn v. Plant Guards*, 383 U.S. 53 (1966), in that they were made with knowledge that they were false or with reckless disregard for their truth or falsity. Finally, Respondent argues that Sanzone and Spinella's comments lost the protection of the Act under the *Atlantic Steel* analysis.

The evidence here establishes that the General Counsel has satisfied the *Burnup & Sims* standard, and that Sanzone and Spinella's participation in the Facebook discussion did not lose its protected status under *Atlantic Steel*, *Jefferson Standard*, or *Linn*. The evidence further establishes that, with respect to Respondent's other asserted reasons for the discharges, the General Counsel has established a prima facie case that Sanzone and Spinella were discharged in retaliation for their protected concerted activity. Finally, Respondent has not met its burden to show by a preponderance of the evidence that Sanzone and Spinella were in fact discharged for legitimate, nondiscriminatory reasons.

2. Sanzone and Spinella engaged in protected concerted activity by participating in the discussion on LaFrance's Facebook account

The evidence establishes that Sanzone and Spinella were engaged in concerted activity within the meaning of Section 7 of the Act when they participated in the discussion on LaFrance's Facebook account. Section 7 of the Act provides that “employees shall have the right to self organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.” It is beyond question that issues related to wages, including the tax treatment of earnings, are directly related to the employment relationship, and may form the basis for protected concerted activity within the meaning of Section 7. See, e.g., *Coram Pond Diner*, 248 NLRB 1158, 1159–1160, 1162 (1980) (protected concerted activity involving employee complaint regarding employer's failure to deduct taxes from pay and provide W-2 forms). While LaFrance herself was a former employee and two customers posted comments as well, current employees Parent and Baumbach, as well as Sanzone and Spinella, were involved in the discussion.

The evidence also establishes that the Facebook discussion was part of a sequence of events, including other, face-to-face employee conversations, all concerned with employees' complaints regarding Respondent's tax treatment of their earnings. It is well settled that concerted activity “encompasses those circumstances where individual employees seek to initiate or to induce or to prepare for group action.” *Worldmark by Wyndham*, 356 NLRB No. 104, slip op. at 2 (2011), quoting *Meyers Industries*, 281 NLRB 882, 887 (1986), enfd. sub nom. *Prill v. NLRB*, 835 F.2d 1481 (D.C. Cir. 1987); see also *KNTV, Inc.*, 319 NLRB 447, 450 (1995) (“Concerted activity encompasses activity which begins with only a speaker and listener, if that activity appears calculated to induce, prepare for, or otherwise relate to some kind of group action.”). The specific medium in which the discussion takes place is irrelevant to its protected nature. See, e.g., *Timekeeping Systems, Inc.*, 323 NLRB 244, 247 (1997) (email regarding vacation policy sent by employees to fellow employees and to management concerted activity).

The record here establishes that prior to the Facebook discussion several employees, including Sanzone, had spoken at the restaurant about Respondent's calculation of their tax withholdings, and that a number of them owed a tax payment to the State of Connecticut after filing their 2010 tax returns. Indeed, DelBuono and Daddona were aware that this was an important issue for a number of the employees, and had as a result scheduled a meeting between the employees and Respondent's payroll administrator for the week after Sanzone and Spinella were discharged. The employees who posted comments on LaFrance's Facebook account specifically discussed the issues they intended to raise at this upcoming meeting and avenues for possible complaints to government entities. As a result, I find that the employees' Facebook discussion was part of an ongoing sequence of events involving their withholdings and taxes owed to the State of Connecticut, and was therefore concerted activity. See, e.g., *Tampa Tribune*, 351 NLRB 1324, 1325

(2007), enf. denied 560 F.3d 181 (4th Cir. 2009) (single conversation concerted when “part of an ongoing collective dialogue” between respondent and its employees and a “logical outgrowth” of prior concerted activity); *Circle K Corp.*, 305 NLRB 932, 933–934 (1991), enf. 989 F.2d 498 (6th Cir. 1993) (“invitation to group action” concerted activity regardless of its outcome).

I further find that Spinella’s selecting the “Like” option on LaFrance’s Facebook account constituted participation in the discussion that was sufficiently meaningful as to rise to the level of concerted activity. Spinella’s selecting the “Like” option, so that the words “Vincent VinnyCenz Spinella . . . like[s] this” appeared on the account, constituted, in the context of Facebook communications, an assent to the comments being made, and a meaningful contribution to the discussion. In fact, Spinella’s indicating that he “liked” the conversation was sufficiently important to engender the meeting with DelBuono and Daddona which ended with his discharge. In addition, the Board has never parsed the participation of individual employees in otherwise concerted conversations, or deemed the protections of Section 7 to be contingent upon their level of engagement or enthusiasm. Indeed, so long as the topic is related to the employment relationship and group action, only a “speaker and a listener” is required. *KNTV, Inc.*, 319 NLRB at 450. I find therefore that Spinella’s selecting the “Like” option, in the context of the Facebook conversation, constituted concerted activity as well.

I find that Sanzone and Spinella’s Facebook comments were not sufficiently egregious as to lose the protection of the Act under *Atlantic Steel* and its progeny.⁵ The *Atlantic Steel* analysis requires the consideration of four factors: (i) the place of the discussion; (ii) the discussion’s subject matter; (iii) the nature of the outburst on the part of the employee; and (iv) whether the outburst was provoked by the employer’s unfair labor practices. See, e.g., *Plaza Auto Center, Inc.*, above at 495, citing *Atlantic Steel*, 245 NLRB at 816. These four criteria are intended to permit “some latitude for impulsive conduct by employees” during protected concerted activity, while acknowledging the employer’s “legitimate need to maintain order.” *Plaza Auto Center, Inc.*, 355 NLRB at 495. As the Board has stated, the protections of Section 7 must “take into account the realities of industrial life and the fact that disputes over wages, bonuses, and working conditions are among the disputes most likely to engender ill feelings and strong responses.” *Consumers Power Co.*, 282 NLRB 131, 132 (1986). Therefore, statements during otherwise protected activity lose the Act’s protection only where they are “so violent or of such serious character as to render the employee unfit for further service.” *St. Margaret Mercy Healthcare Centers*, 350 NLRB 203, 204–

205 (2007), enf. 519 F.3d 373 (7th Cir. 2008), quoting *Dreis & Krump Mfg. Co. v. NLRB*, 544 F.2d 320, 329 (7th Cir. 1976).

In order to apply the *Atlantic Steel* analysis, the specific statements at issue must be determined. Sanzone posted one comment on LaFrance’s Facebook account: “I owe too. Such an asshole.” Although Sanzone testified that she was using the word “asshole” to refer to the fact that she owed tax monies to the State of Connecticut, I find that the more plausible conclusion is that she was in fact referring to Ralph DelBuono, who was responsible for Respondent’s accounting, and is discussed by LaFrance. Spinella clicked the “Like” option, resulting in the statement “Vincent VinnyCenz Spinella and . . . like this,” which refers in the context of a Facebook discussion to the entire topic as it existed at the time.

I reject Respondent’s contention that Sanzone and Spinella may be deemed responsible for comments that they did not specifically post, such as those of LaFrance. Respondent makes much of the fact that it did not discharge the other two employees—Danielle Marie Parent and Sarah Baumbach—who participated in the discussion, contending that this illustrates that Sanzone and Spinella’s comments lost the Act’s protection. Such an argument is not meaningful within the context of the *Atlantic Steel* analysis, and evidence that some employees involved in protected concerted activity were not subject to retaliation generally carries little weight in the *Wright Line* context. In any event, Respondent makes no attempt to explain why Parent and Baumbach should not be charged with having adopted LaFrance’s comments, as were Sanzone and Spinella. In addition, the Board has emphasized that when evaluating the conduct of individual employees engaged in a single incident of concerted activity, each employee’s specific conduct must be analyzed separately. *Crowne Plaza LaGuardia*, 357 NLRB No. 95, slip op. at 4–6 (2011) (only employees that deliberately attempted to physically restrain manager lost Sec. 7’s protection; other employees involved in confrontation were unlawfully discharged). As a result, the two comments under consideration are Sanzone’s remark, “I owe too. Such an asshole.” and Spinella’s statement “Vincent VinnyCenz Spinella [and] like this.”

The first of the *Atlantic Steel* factors—the place of the discussion—mitigates in favor of a finding that Sanzone and Spinella’s comments did not lose the protection of the Act. The comments occurred during a Facebook conversation, and not at the workplace itself, so there is no possibility that the discussion would have disrupted Respondent’s work environment. *Datwyler Rubber & Plastics, Inc.*, 350 NLRB at 670 (outburst which took place during a meeting in the employee breakroom not disruptive to employer’s work processes). Because DelBuono and Respondent’s other owners were not present, there was no direct confrontational challenge to their managerial authority.

The evidence does establish, as Respondent contends, that two of its customers participated in the Facebook conversation. However, I find that this fact is insufficient to remove Sanzone and Spinella’s comments from the protection of the Act. The Board has held that the presence of customers during brief episodes of impulsive behavior in the midst of otherwise protected activity is insufficient to remove the activity from the ambit of

⁵ Contrary to Respondent’s contention in its posthearing brief, the *Atlantic Steel* analysis is not limited to statements made during formal grievance proceedings. See, e.g., *Plaza Auto Center, Inc.*, 355 NLRB at 493, 495 (statement made during meeting between employee and managers in nonunionized workplace); *Datwyler Rubber & Plastics, Inc.*, 350 NLRB 669, 669–670 (2007) (outburst occurred during employee meeting).

Section 7's protection where there is no evidence of disruption to the customers. *Crowne Plaza LaGuardia*, 357 NLRB No. 95, slip op. at 6 (presence of two hotel guests during employees' loud chanting and confrontation with manager insufficient to divest activity of statutory protection without evidence that services were disrupted); *Goya Foods of Florida*, 347 NLRB 1118, 1134 (2006), enfd. 525 F.3d 1117 (11th Cir. 2008) (brief episode of shouting inside supermarket insufficient to render activity unprotected in absence of evidence of customer disruption). In addition, the activity at issue here did not take place at Respondent's restaurant, but on the Facebook account of a former employee, whom customers would have to specifically locate and "befriend" in order to view. As a result, the situation at issue here is materially different from conduct occurring in an employer's establishment, which customers engaged in ordinary business transactions with the employer would be forced to witness. Finally, there is no evidence that the Facebook discussion somehow generally disrupted Respondent's customer relationships. Although Daddona testified that he had not seen one of the customers who participated in the conversation since that time, there is no evidence as to why this customer had not visited the restaurant. In fact, the other customer who participated in the conversation stated that in his opinion the restaurant was too expensive. As a result, there is insufficient evidence to find that Sanzone and Spinella's comments resulted in some sort of harm to Respondent's business.

For all of the foregoing reasons, I find that the first component of the *Atlantic Steel* analysis militates in favor of a finding that Sanzone and Spinella's participation in the Facebook discussion did not lose its protected character.

With respect to the second aspect of the *Atlantic Steel* analysis, the subject matter of the discussion, the evidence establishes that the Facebook conversation generally addressed the calculation of taxes on the employees' earnings by Respondent, and the fact that many of the employees ended up owing money to the State of Connecticut after filing their 2010 tax returns. Because the subject matter of the conversation involved and protected concerted activity, this factor militates in favor of a finding that Sanzone and Spinella's activity remained protected under the Act. *Plaza Auto Center, Inc.*, 355 NLRB at 495 (discussion involving intemperate comments addressed protected concerted activity pertaining to compensation).

As to the third factor, the nature of Sanzone and Spinella's "outburst" clearly did not divest their activity of the Act's protection under the *Atlantic Steel* line of cases. First of all, the comments were not made directly to DelBuono or Daddona, and did not involve any threats, insubordination, or physically intimidating conduct. See *Plaza Auto Center*, above at 496–497 (nature of outburst "not so opprobrious" as to deprive employee of statutory protection where no evidence of physical harm or threatening conduct); *Tampa Tribune*, 351 NLRB at 1326 (employee's outburst remained protected where not directed at manager and unaccompanied by physical conduct, threats, or confrontational behavior). Spinella's comment contained no profanity, and Sanzone's use of the word "asshole" to describe DelBuono is clearly insufficient to divest her activity

of the Act's protection.⁶ See *Plaza Auto Center*, above at 495–498 (employee referred to owner as a "f—king motherfucker," "f—king crook," and "asshole"); *Tampa Tribune*, 351 NLRB at 1324–1325 (employee called vice president a "stupid f—king moron"); see also *Alcoa, Inc.*, 352 NLRB 1222, 1225–1226 (2008) (employee referred to supervisor as an "egotistical f—ker"); *Burle Industries*, 300 NLRB 498 (1990), enfd. 932 F.2d 958 (3d Cir. 1991) (employee called supervisor a "f—king asshole").

Respondent contends that Sanzone and Spinella's remarks also lost the Act's protection in that they were disparaging and disloyal statements within the meaning of *NLRB v. Electrical Workers Local 1229 (Jefferson Standard)*, 346 U.S. 464 (1953). In that case, employee statements were found unprotected where they were made "at a critical time in the initiation of the company's business," were unrelated to any ongoing labor dispute, and constituted "a sharp, public, disparaging attack upon the quality of a company's product and its business policies, in a manner reasonably calculated to harm the company's reputation and reduce its income." *Electrical Workers Local 1229 (Jefferson Standard)*, 346 U.S. at 472; see also *Santa Barbara News-Press*, 357 NLRB No. 51, slip op. at 3–4 (2011); *MasTec Advanced Technologies*, 357 NLRB No. 17, slip op. at 5 (2011); *Valley Hospital Medical Center*, 351 NLRB 1250, 1252 (2007), enfd. 188 LRRM 2384 (9th Cir. 2009). The Board has cautioned that "disparagement of an employer's product" and "the airing of what may be highly sensitive issues" must be carefully distinguished. *Valley Hospital Medical Center*, 351 NLRB at 1252. In order to lose the Act's protection, public criticism of the employer must be made with a "malicious motive." *Id.* In this respect, the Board has held that statements are "maliciously untrue" when "made with knowledge of their falsity or with reckless disregard for their truth or falsity."⁷ *MasTec Advanced Technologies*, 357 NLRB No. 17, slip op. at 5. The fact that statements are "false, misleading, or inaccurate" is not sufficient to establish that they are maliciously untrue. *Id.*; see also *Valley Hospital Medical Center*, 351 NLRB at 1252.

As an initial matter, however, I find that the statements made by Sanzone and Spinella here never lost the Act's protection, in that they were not susceptible to a defamatory meaning under the relevant caselaw. It is axiomatic that prior to considering issues of reckless or knowing falsity, "there must be a false statement of fact." *DHL Express, Inc.*, 355 NLRB 680, 680 fn. 3, 695 (2010), quoting *Steam Press Holdings v. Hawaii Team-*

⁶ The epithet "shady little man" is also clearly insufficient to divest a statement from the protection of the Act under the *Atlantic Steel* line of cases, even in the event that Sanzone and Spinella could be deemed to have adopted this comment of LaFrance's.

⁷ As Respondent discusses in its post-hearing brief, the Supreme Court has also applied this standard, originating in *New York Times v. Sullivan*, 376 U.S. 254 (1964), to actions for defamation involving labor disputes and other conduct protected by the Act. See *Linn v. Plant Guards*, 383 U.S. 53, 64–65 (1966) (State law defamation actions based upon statements made in the course of a labor dispute permissible where the plaintiff can show that the defamatory statements were made with malice and caused damages); see also *Old Dominion Branch No. 496, Letter Carriers v. Austin*, 418 U.S. 264, 273 (1974).

sters *Local 996*, 302 F.3d 998, 1009 fn. 6 (9th Cir. 2002). The Board and the courts have long recognized that in the context of a labor dispute, statements may be “hyperbolic,” biased, “vehement,” “caustic,” and may even involve a “vigorous epithet,” while retaining the Act’s protection. *DHL Express, Inc.*, 355 NLRB 680, quoting *Joliff v. NLRB*, 513 F.3d 600, 609–610 (6th Cir. 2008); see also *Valley Hospital Medical Center*, 351 NLRB at 1253. Sanzone’s statement, “I owe to . . . such an asshole,” accurately reflects the fact that she did owe a tax payment to the State of Connecticut, and her referring to DelBuono as an “asshole” constitutes an epithet, as opposed to an assertion of fact. *Joliff*, 513 F.3d at 609–610; see also *Moriarty v. Lippe*, 162 Conn. 371, 294 A.2d 326 (Conn. 1972) (epithets such as “big fat oaf,” “son of a bitch” and other “words of general abuse” are not slanderous per se, and require proof of special damages for recovery). Spinella’s statement “Vincent VinnyCenz Spinella . . . like[s] this” is also not a statement of fact with respect to Respondent or DelBuono. As a result, Sanzone and Spinella’s statements are not even potentially defamatory, and did not lose the protection of the Act under the *Jefferson Standard* line of cases. I would reach the same conclusion even if I found that Sanzone and Spinella had somehow adopted the comments of LaFrance and the other employees. See *Steam Press Holdings, Inc.*, 302 F.2d at 1002, 1005–1009 (accusations that company’s owner was “making money” and “hiding money,” which belied employer’s asserted poor financial condition during negotiations, were not fact statements susceptible to a defamatory meaning).

I also find that the statements made by Sanzone and Spinella were not deliberately false, or made with reckless disregard for their truth or falsity, even assuming they somehow adopted LaFrance’s comments that DelBuono “fucked up the paperwork,” was “a shady little man,” and “probably pocketed [the tax deductions] from all our paychecks.” There is no real dispute that DelBuono was responsible for Respondent’s accounting, and that many of Respondent’s employees owed taxes to the State of Connecticut after filing their 2010 tax returns. Indeed, the evidence establishes that the problem was so widespread, and had caused such consternation among Respondent’s employees, that a meeting had been arranged with representatives from the payroll service used by Respondent for the following week. In addition, Sanzone testified that her paycheck only reflected 40 hours of work per week regardless of her actual work hours, and that she was sometimes paid in cash for work in excess of 40 hours per week, and sometimes not paid at all for overtime hours. While DelBuono generally denied this during his testimony, Respondent provided no other meaningful evidence to rebut Sanzone’s assertions.

Given the requirement of malice, the Board considers the perspective of the employee in order to determine whether statements, regardless of their actual truth, were made with knowledge that they were false or with reckless disregard for their truth or falsity. *MasTec Advanced Technologies*, 357 NLRB No. 17, slip op. at 5 (statements in dispute “fairly reflected [employees’] personal experiences” and were therefore not made maliciously); *Valley Hospital Medical Center*, 351 NLRB at 1253 (statements not maliciously false where they were based on employee’s “own experiences and the experi-

ences of other nurses as related to [employee]”). Assuming LaFrance’s comments were adopted by Sanzone and Spinella, the evidence establishes that, given the employees’ direct experience with their 2010 tax returns and Respondent’s other payroll practices, they were not malicious. While they might be considered “hyperbolic,” the evidence does not establish that they were made with knowledge of their falsity or reckless disregard for the truth. See, e.g., *Asplundh Tree Expert Co.*, 336 NLRB 1106, 1108 (2001), vacated on other grounds 365 F.3d 168 (3d Cir. 2004) (employee’s statement that supervisor had “pocketed” the difference between employees’ per diem and actual hotel expenses protected); *Mediplex of Wethersfield*, 320 NLRB 510, 513 (1995) (accusation that employer had “cheated” employees through paid time off program protected); *KBO, Inc.*, 315 NLRB 570 (1994), enfd. 96 F.3d 1448 (6th Cir. 1996) (statement that employer was “taking money out of the employees’ profit-sharing accounts to pay the lawyers to fight the Union” protected).

In addition, the evidence establishes that Sanzone and Spinella’s statements were not directed to the public as part of a campaign to raise public awareness of the employees’ dispute with Respondent. Other cases applying the *Jefferson Standard* analysis involve the deliberate dissemination of allegedly disparaging statements through the news media, or as part of a campaign specifically directed to the public at large. See, e.g., *MasTec Advanced Technologies*, 357 NLRB No. 17 slip op. at 3–4 (statements made on news broadcast); *Valley Hospital Medical Center*, 351 NLRB at 1250–1251, 1253–1254 (statements made at press conference organized by the union, on a website maintained by the union and accessible to the general public, and in a flyer distributed to the public by the union in front of the employer’s facility). Here, by contrast, Sanzone, Spinella, and LaFrance’s comments were posted on LaFrance’s Facebook account, which was not accessible to the general public. Instead, each person wishing to view the account (including customers of Respondent) needed to obtain LaFrance’s specific permission through an accepted request to become her “Friend.” This militates against a finding that the statements made during the Facebook discussion were made with a malicious intent to injure Respondent’s business and DelBuono’s reputation in the eye of the general public. The more reasonable conclusion is that the participants were, in LaFrance’s words, “venting” their frustration with one another regarding the tax withholding situation and discussing the upcoming meeting with representatives from Respondent’s payroll service.

The other factors considered as part of the *Jefferson Standard* analysis also do not support a conclusion that Sanzone and Spinella’s statements on LaFrance’s Facebook account lost the protection of the Act. There is no evidence that the statements were made at a critical time during the initiation of the employer’s business; Respondent’s restaurant and bar had been operating since December 2009. The statements were directly related to the ongoing dispute between the employees and Respondent’s management regarding the tax treatment of the employees’ earnings, which had resulted in a number of the employees’ owing taxes to the State of Connecticut. They were not a gratuitous attempt to injure Respondent’s business. Finally,

Sanzone and Spinella's statements were not an attack on Respondent's product. They did not address, for example, the quality of the food, beverages, services, or entertainment at Respondent's restaurant and bar,⁸ but were solely related to the employees' owing taxes to the State.

For all of the foregoing reasons, I find that the third component of the *Atlantic Steel* analysis—the nature of the outburst—indicates that Sanzone and Spinella's statements did not lose their protected character.

As for the fourth of the *Atlantic Steel* criteria, whether the outburst was provoked by Respondent's unfair labor practices, General Counsel does not contend that Sanzone and Spinella's Facebook statements were provoked by any unfair labor practice of Respondent. Therefore, this component of the analysis militates in favor of a finding that Sanzone and Spinella's statements were not protected. However, in that I have concluded that factors one, two, and three of the *Atlantic Steel* standard support a finding that Sanzone and Spinella's Facebook comments did not lose the protection of the Act, I find that they remained protected concerted activity.

3. Sanzone and Spinella's discharges were unlawful under the *Burnup & Sims* standard

As discussed above, the *Burnup & Sims* analysis involves the application of four factors: (i) whether the discharged employee was engaged in protected activity at the time of their purported misconduct; (ii) whether the employer knew of the protected activity; (iii) whether the basis for the discharge was the employee's alleged misconduct in the course of their protected activity; and (iv) whether the employee was actually guilty of the misconduct. When the evidence establishes that the employee was discharged based on alleged misconduct occurring in the course of protected activity, the burden shifts to the respondent to show that "it had an honest or good-faith belief that the employee engaged in the misconduct." *Alta Bates Summit Medical Center*, 357 NLRB No. 31, slip op. at 1–2 (2011); see also *Roadway Express*, 355 NLRB 197, 1015 (2010), enf. 427 Fed. Appx. 838 (11th Cir. 2011). If the respondent does so, the burden then shifts back to the General Counsel to prove that the employee did not actually engage in the alleged misconduct. *Alta Bates Summit Medical Center*, 357 NLRB No. 31, slip op. at 2; *Roadway Express*, 355 NLRB at 1015.

The evidence establishes here, as discussed above, that Sanzone and Spinella were engaged in protected concerted activity—the discussion with other employees of Respondent's calculation of their tax withholdings—at the time of their alleged misconduct. The record also establishes that Respondent knew of this protected activity at the time that Sanzone and Spinella were discharged. Daddona testified that his sister informed him of the Facebook discussion on LaFrance's account, and that he viewed the discussion with DelBuono, prior

to Sanzone and Spinella's discharge. In fact, Respondent admits that it discharged Sanzone in part for her comments, and as discussed below DelBuono testified that he initiated the meeting during which Spinella was discharged specifically to confront him about his having selected the "Like" option. Therefore, the first two components of the *Burnup & Sims* analysis are satisfied.

I also find that the evidence establishes that Sanzone and Spinella were discharged for alleged misconduct in the course of their protected activity, the third criterion of the *Burnup & Sims* analysis. Respondent admits that Sanzone was discharged for "disloyalty," comprised in part of her comment on LaFrance's Facebook account.⁹ However, Respondent contends that Spinella was discharged for poor work performance, including failing to stock deliveries, unauthorized cigarette breaks, and excessive cell phone use and socializing with other staff. The evidence does not substantiate this contention. While Daddona testified that Spinella was not discharged because of his having selected the "Like" option on LaFrance's Facebook account, and that his having done so was not discussed during the meeting which culminated in his discharge, DelBuono thoroughly contradicted these assertions. Thus, DelBuono testified that he and Daddona decided to confront Spinella because his "Facebook comment raised a red flag" that he was not happy working for Respondent. DelBuono testified that during the meeting he told Spinella that he was obviously not happy, and "questioned him" regarding the Facebook discussion, asking him, "if he liked those defamatory and derogatory statements so much well why is he still working for us?" DelBuono stated that he then told Spinella that because he "liked the disparaging and defamatory comments," it was "apparent" that Spinella wanted to work somewhere else. I therefore find based on DelBuono's testimony that Spinella was discharged because of his having selected the "Like" option on LaFrance's Facebook account, and that both he and Sanzone were discharged for alleged misconduct occurring in the course of their protected activity.

Finally, as discussed above, I have found that Sanzone and Spinella's comments did not lose the Act's protection under the four *Atlantic Steel* factors, and that they did not lose the protection of the Act under the *Jefferson Standard* analysis, in that they were not made with knowledge of their falsity or with reckless disregard for their falsity or truth. I therefore find that regardless of the character of any belief regarding misconduct held by Daddona and DelBuono, Sanzone and Spinella did not in fact commit misconduct by virtue of their participating in the discussion on LaFrance's Facebook account.

For all of the foregoing reasons, I find under *Burnup & Sims* that Respondent violated Section 8(a)(1) of the Act by discharging Sanzone and Spinella.

⁸ Indeed, the sole comment of this nature was offered, unsolicited, by customer Jonathan Feeley, who stated that Respondent's restaurant and bar were "way too expensive." Customer DeSantis stated, "Yeah I really don't go to that place anymore," but there is no evidence to establish why. In fact, because he made this comment during the discussion on LaFrance's Facebook account, he had presumably stopped frequenting Respondent's restaurant prior to that time.

⁹ For the reasons discussed in sec. 4 regarding Respondent's asserted reasons for Sanzone and Spinella's discharges based on work performance under *Wright Line*, I find that Sanzone was not discharged for reasons relating to cash register inaccuracies.

4. Respondent's *Wright Line* defenses

In addition to its arguments regarding the nonprotected nature of Sanzone and Spinella's participation in the Facebook discussion, Respondent asserts reasons for Sanzone and Spinella's discharges based upon their work performance, and unrelated to their protected concerted activity. Respondent contends that Sanzone was discharged for repeated cash register inaccuracies, and that Spinella was discharged for poor work performance involving a number of issues. To the extent that Respondent has raised issues regarding its motivation for the discharges, I will analyze these contentions within the framework articulated in *Wright Line*, 251 NLRB 1083 (1980), *enfd.* 662 F.2d 899 (1st Cir. 1981), *cert denied* 455 U.S. 989 (1982), *approved in NLRB v. Transportation Management Corp.*, 462 U.S. 393 (1983).

To establish an unlawful discharge under *Wright Line*, the General Counsel must prove that the employee's protected conduct was a motivating factor in the employer's decision to take action against them by proving the employee's protected activity, employer knowledge of that activity, and animus against the employee's protected conduct. *Manno Electric, Inc.*, 321 NLRB 278, 280 (1996); *Naomi Knitting Plant*, 328 NLRB 1279, 1281 (1999). The burden of persuasion then shifts to the employer to show that it would have taken the same action even in the absence of the protected conduct. *Wright Line*, 251 at 1089; *Septix Waste, Inc.*, 346 NLRB 494, 496 (2006); *Williamette Industries*, 341 NLRB 560, 563 (2004). Respondent must persuade by a preponderance of the credible evidence that it would have taken the same action in the absence of the protected conduct. *T&J Trucking Co.*, 316 NLRB 771 (1995); *Manno Electric, Inc.*, 321 NLRB at 280 fn. 12 (1996).

I find that General Counsel has established a *prima facie* showing that Sanzone and Spinella's protected concerted activity was a motivating factor in their discharges. As discussed above, Sanzone and Spinella's participation in the Facebook discussion remained protected activity throughout, and there is no question that at the time they were discharged Daddona and DelBuono were aware of their comments. Animus against their protected activity is evinced by the timing of their discharges immediately after the Facebook discussion, and Daddona and DelBuono's comments while discharging them, some of which, as addressed below, constitute independent violations of Section 8(a)(1). See, e.g., *Manorcare Health Services-Easton*, 356 NLRB No. 39, slip op. at 3, 25 (2010), *enfd.* 661 F.3d 1139 (D.C. Cir. 2011) (discipline of employee "just days" after initial public support for the union indicative of unlawful motivation); *Austal USA, LLC*, 356 NLRB No. 65, slip op. at 1-2 (2010) (8(a)(1) violations constitute evidence of animus).

The evidence presented here is insufficient to satisfy Respondent's burden to show that it discharged either Sanzone or Spinella for legitimate, non-discriminatory reasons. Respondent's asserted work-performance reasons for discharging Spinella are utterly unsubstantiated by the record. Both Daddona and DelBuono generally testified that Spinella failed to restock supplies in a timely manner, socialized excessively with waitresses, and took too many breaks to smoke cigarettes and use his cell phone. However, DelBuono testified that what

"raised a red flag" and immediately precipitated the meeting which culminated in Spinella's discharge was his having selected the "Like" option on LaFrance's Facebook account. According to DelBuono, he then "questioned" Spinella regarding the Facebook conversation before asking him why he was still working for Respondent; the evidence does not establish that Spinella's various performance problems were even touched upon during this meeting. Given DelBuono's testimony, Daddona's testimony that the Facebook discussion was not mentioned during the meeting and played no role in Respondent's reasons for discharging Spinella is obviously not worthy of belief, and undermines his credibility as a witness overall.

Other factors also contradict Respondent's assertion that it discharged Spinella for work performance problems. Daddona testified that he first noticed Spinella's poor work habits during the first 2 months of his employment, and discussed them with him on a minimum of six occasions. Although I do not find Daddona to be a credible witness, Spinella did testify that Daddona and DelBuono had a number of informal conversations with him and the other kitchen workers, which included suggestions for improvement. However, there is no evidence that Respondent issued written discipline to Spinella, and no evidence that Spinella was ever informed in any way that failure to improve would result in discharge. Crediting Spinella's testimony, I find that DelBuono and Daddona's discussions with him failed to rise to the level of meaningful disciplinary action. In any event, it is also well settled that the imposition of discipline for conduct that has been tolerated or condoned constitutes evidence of unlawful motivation. See, e.g., *Air Flow Equipment, Inc.*, 340 NLRB 415, 419 (2003). As a result, I find that Respondent has failed to substantiate its contention that Spinella was discharged for work performance problems, as opposed to his protected participation in the Facebook discussion.

With respect to Respondent's assertion that Sanzone was discharged in part for cash register inaccuracies, the credible evidence establishes that Daddona informed her on one occasion that her cash drawer was short after a bartending shift some time in the fall of 2010. I do not credit Daddona's assertion that her cash drawer "somewhat regularly" contained funds in excess of what could be accounted for through sales at the end of her bartending shifts, which he purportedly first discovered in August 2010. Daddona claims he was told by a business acquaintance that this might mean that Sanzone was recording fewer drinks than were actually purchased by customers, and in effect stealing the difference. If this is the case, it is implausible that Respondent would not have taken more immediate action to discharge Sanzone given the direct impact on its business and the egregious nature of potential theft. The evidence also establishes that Sanzone received a raise in November 2010 and a Christmas bonus that same year, actions which no reasonable employer would take if it truly believed that she was possibly engaged in theft. Respondent also failed to offer a shred of documentary evidence to substantiate its contention that Sanzone's cash drawer regularly contained an overage of funds. Indeed, DelBuono, who has overall responsibility for Respondent's accounting, was not even questioned regarding this asserted reason for Sanzone's discharge. As a result, I find

that Respondent has failed to provide adequate evidence to substantiate its contention that Sanzone was discharged for cash register inaccuracies, as opposed to her comment during the discussion on LaFrance's Facebook account.

For all of the foregoing reasons, I find that Respondent has failed to meet its burden to establish that it discharged Sanzone and Spinella for legitimate, nondiscriminatory reasons. I therefore find that Sanzone and Spinella's discharges violated Section 8(a)(1).

B. Threats to Initiate Legal Action

The consolidated complaint alleges that Respondent threatened employees with legal action in violation of Section 8(a)(1) on February 3 and 4. There is no dispute that Respondent's attorney and admitted agent, Joseph Yamin, wrote to Sanzone on February 4, threatening to institute a defamation action against her if she did not retract her statement on LaFrance's Facebook account. Sanzone had LaFrance delete her comment, and sent a letter to Yamin stating that her comment had been erased. Yamin then wrote to Sanzone stating that she was required to post a "formal statement that the defamatory statements were untrue," and demanded written proof that she had done so. Sanzone did not respond, and did not hear from Yamin again.

The evidence overall also establishes that Respondent threatened Spinella with legal action on February 3, as alleged in the consolidated complaint. I credit Spinella's testimony that as he was leaving the discharge meeting with Daddona and DelBuono on February 3, DelBuono stated that Spinella would be hearing from Respondent's lawyers. Daddona's testimony regarding this meeting is simply not believable, as he contended that Spinella's participation in the Facebook conversation was never discussed. DelBuono's testimony is more credible, as he admitted to "questioning" Spinella regarding the Facebook discussion, including asking Spinella "why is he still working for us?" given his affinity for "the disparaging and defamatory comments." Given DelBuono's corroboration of Spinella's account in this regard, and Respondent's written threat, by its attorney, to initiate an action against Sanzone, I credit Spinella's statement that DelBuono told him as he left the February 3 meeting that he would hear from Respondent's attorney. Given DelBuono's statements during the meeting that the comments were defamatory, and that his attorney had advised him to discharge anyone involved for that reason, Spinella would reasonably have interpreted DelBuono's statement that he would hear from Respondent's attorney as a threat of legal action.

There is no dispute that Respondent never filed an action for defamation against Sanzone, Spinella, or LaFrance.

The General Counsel contends that Respondent's threats to sue Sanzone and Spinella for defamation violated Section 8(a)(1), in that they reasonably tended to interfere with, restrain, and coerce them in the exercise of their Section 7 rights. *DHL Express, Inc.*, 355 NLRB 680 fn. 3, 692–694 (2010); see also *Network Dynamics Cabling*, 351 NLRB 1423, 1425 (2007); *Postal Service*, 350 NLRB 125, 125–126 (2007), *enfd.* 526 F.3d 729 (11th Cir. 2008). Respondent argues that its correspondence with Sanzone was permissible in that the filing

and prosecution of a well-founded lawsuit does not violate Section 8(a)(1) even if initiated with a retaliatory motive, citing *Bill Johnson's Restaurants v. NLRB*, 461 U.S. 731 (1983). Respondent contends that an action for defamation against Sanzone would have had a reasonable basis, and therefore Respondent's threats to initiate one did not violate Section 8(a)(1).¹⁰

The Board has consistently held that threats to bring legal action against employees for engaging in protected concerted activity violate Section 8(a)(1), in that they reasonably tend to interfere with, restrain, and coerce employees in the exercise of their Section 7 rights. *DHL Express, Inc.*, 355 NLRB 680 fn. 3, 692, citing *S.E. Nichols Marcy Corp.*, 229 NLRB 75 (1977). In *BE & K Construction Co.*, 351 NLRB 451 (2007), the Board held that retaliatory but reasonably based lawsuits do not violate Section 8(a)(1). However, the Board has explicitly declined to apply this standard to threats to initiate litigation, even where they are "incidental" to the actual filing of the lawsuit itself. *Postal Service*, 350 NLRB at 125–126; see also *DHL Express, Inc.*, 355 NLRB 680 fn. 3. In addition, the Board has repeatedly held that, even if it had determined that the *BE & K* standard applied to threats of litigation "incidental" to the filing of a lawsuit, such threats cannot be considered "incidental" to litigation where, as here, a lawsuit was never filed.¹¹ *DHL Express, Inc.*, 355 NLRB 680 fn. 3; *Postal Service*, 350 NLRB at 125–126. As a result, I find that the *BE & K* standard is inapplicable.

As discussed in section A,2 above, I find that Sanzone and Spinella's statements were not defamatory, and were not made with knowledge of their falsity or with reckless disregard for their truth or falsity. *DHL Express, Inc.*, 355 NLRB at 692. I therefore find, as discussed above, that their participation in the Facebook conversation never lost the Act's protection.

As a result, the evidence establishes that Respondent's repeated threats to bring legal action against Sanzone and Spinella would reasonably tend to interfere with, restrain, and coerce them in the exercise of their Section 7 rights. Indeed, Sanzone had LaFrance remove her statement from the Facebook account, and Spinella returned to the account to select the "Unlike" option. Even after Sanzone did so, Respondent's attorney wrote to her again demanding written proof that she had made "a formal statement" that her previous remark was "untrue." See *DHL Express, Inc.*, 355 NLRB at 693–694 (threat to initiate legal action coercive where never retracted, even after "the allegedly offensive statements were corrected"). Sanzone and Spinella's responses to Respondent's threats of litigation, and Respondent's subsequent insistence on pursuing the matter through its attorney, further indicate that its conduct was impermissibly coercive. Thus I find that Respondent violated Section 8(a)(1) of the Act by threatening Sanzone and

¹⁰ Respondent does not advance any argument regarding DelBuono's threat to take legal action against Spinella.

¹¹ Sanzone's written response to Yamin's February 4 letter stating that she had had LaFrance remove her remark from LaFrance's Facebook account further supports the conclusion that the threat to initiate legal action against her was not "incidental" to the filing of a lawsuit. See *Network Dynamics Cabling*, 350 NLRB at 1427 fn. 14.

Spinella with legal action in retaliation for their protected concerted activity.

*C. Other Statements by Daddona and DelBuono
Allegedly Violating Section 8(a)(1)*

The consolidated complaint alleges that Respondent also violated Section 8(a)(1) on February 2, when Daddona informed employees that they were discharged because of their protected concerted activities, and on February 3, when DelBuono interrogated employees regarding their protected concerted activities and threatened employees with discharge for that reason. I find that the evidence establishes that Respondent committed these additional violations of Section 8(a)(1).

Sanzone testified that while discharging her on February 2, Daddona stated that she “wasn’t loyal enough to be working at Triple Play anymore,” because of her comment on LaFrance’s Facebook account. Daddona admitted that Sanzone was discharged because “her loyalty was not to us” after “we saw what was going on on Facebook and with the drawer;” however, he did not testify regarding his actual conversation discharging Sanzone. Because Sanzone’s account is therefore not meaningfully rebutted,¹² the record establishes that Daddona told her that she was discharged because she was insufficiently “loyal” to work for Respondent given her comment on Facebook. As Sanzone’s participation in the Facebook discussion constituted protected concerted activity, Daddona’s statement to her that she had been discharged for that reason violated Section 8(a)(1). *Extreme Building Services Corp.*, 349 NLRB 914, 914 fn. 3, 929 (2007) (employer violated Sec. 8(a)(1) by telling an employee he was discharged because of his union membership); *Watts Electric Corp.*, 323 NLRB 734, 735 (1997) (employee unlawfully informed that he had been discharged for distributing union flyers), “revd. in part, vacated in part mem. 166 F.3d 351 (11th Cir. 1998).”

The evidence also establishes that DelBuono coercively interrogated Spinella and unlawfully informed him that those employees who participated in the Facebook discussion would be discharged during their meeting on February 3. DelBuono admitted that he “questioned” Spinella during this meeting, and I credit Spinella’s testimony that DelBuono asked him about the identities of the participants, the significance of the “Like” option, and, as DelBuono testified, “[I]f he liked those defamatory and derogatory statements so much well why is he still working for us?” DelBuono admitted that he told Spinella that it was “apparent” that he wanted to work somewhere else, and given the threats to initiate legal action as discussed above, I credit Spinella’s testimony that DelBuono told him that Respondent’s attorney had advised discharging anyone involved in the Facebook discussion for defamation.

I find that DelBuono’s questioning of Spinella was coercive and therefore unlawful. The Board determines whether questioning regarding protected activity is unlawfully coercive by considering any background of employer hostility, the nature of

the information, the status of the questioner in the employer’s hierarchy, the place and method of questioning, and the truthfulness of the employee’s answer. *Westwood Health Care Center*, 330 NLRB 935, 939 (2000). Here, these factors overall establish that DelBuono’s questioning was impermissibly coercive. DelBuono and Spinella’s conversation was not a casual talk on a shop floor between individuals who had some sort of personal relationship. See *Manor Health Services-Easton*, 356 NLRB No. 39, slip op. at 17 (questioning impermissible where no evidence of personal friendship between agent and employees); compare *Smithfield Packing Co.*, 344 NLRB 1, 2 (2004). DelBuono and Daddona specifically called Spinella into their office for a meeting, and had LaFrance’s Facebook account displayed on the computer. *Manor Health Services-Easton*, 356 NLRB No. 39, slip op. at 18 (questioning coercive where interaction was “neither casual nor accidental”). Sanzone’s discharge the previous day evinces a backdrop of hostility toward the employees’ protected concerted activity. The meeting was characterized by unlawful conduct on the part of DelBuono, including the statement that Respondent’s attorney had advised discharging all employees engaged in the discussion, and DelBuono’s threat to initiate legal action against Spinella for participating in the Facebook conversation. See *Evergreen America Corp.*, 348 NLRB 178, 208 (2006), *enfd.* 531 F.3d 321 (4th Cir. 2008) (questioning accompanied by statements evincing hostility toward union activities more likely to be coercive); *Demco New York Corp.*, 337 NLRB 850, 851 (2002). Finally, the meeting culminated in Spinella’s unlawful discharge. In these circumstances, the truthfulness of Spinella’s responses to DelBuono’s questions is not significant.

I further find that DelBuono’s statement that his attorney had advised him to discharge every employee who participated in the Facebook discussion, which occurred in the context of DelBuono’s repeatedly demanding that Spinella provide a justification for his continued employment, constituted a threat of discharge in violation of Section 8(a)(1). See *White Transfer & Storage Co.*, 241 NLRB 1206, 1209–1210 (1979) (employer’s statement to employees that he “had been with his lawyer all day,” who advised him “that if he had a good enough reason to terminate [employees], to go ahead and do it” unlawful threat of discharge).

For all of the foregoing reasons, I find that Daddona and DelBuono’s statements to Sanzone and Spinella violated Section 8(a)(1) of the Act in the manner described above.

D. Respondent’s Internet/Blogging Policy

It is well settled that an employer’s maintenance of a work rule which reasonably tends to chill employees’ exercise of their Section 7 rights violates Section 8(a)(1) of the Act. *Lafayette Park Hotel*, 326 NLRB 824, 825 (1998), *enfd.* 203 F.3d 52 (D.C. Cir. 1999). A particular work rule which does not explicitly restrict Section 7 activity will be found unlawful where the evidence establishes one of the following: (i) employees would “reasonably construe the rule’s language” to prohibit Section 7 activity; (ii) the rule was “promulgated in response” to union or protected concerted activity; or (iii) “the rule has been applied to restrict the exercise of Section 7 rights.” *Lutheran Heritage Village-Livonia*, 343 NLRB 646,

¹² I decline to draw an adverse inference based upon the failure of Daddona and DelBuono to address certain of the events of Sanzone and Spinella’s discharges during their testimony, as suggested by the General Counsel.

647 (2004). The Board has cautioned that rules must be afforded a “reasonable” interpretation, without “reading particular phrases in isolation” or assuming “improper interference with employee rights.” *Lutheran Heritage Village-Livonia*, 343 NLRB at 646.

The General Counsel contends that Respondent’s Internet/Blogging policy is unlawful, in that it states that employees may be “subject to disciplinary action” for “engaging in inappropriate discussions about the company, management, and/or co-workers.” The General Counsel contends that employees would reasonably construe the language of the policy to restrict Section 7 activity given the breadth of the word “inappropriate,” and of the phrase “the company, management and/or co-workers.” The General Counsel also argues that the rule’s failure to provide concrete examples of prohibited conduct which would lead employees to believe that it applies solely to serious misconduct leaves it susceptible to the interpretation that it encompasses protected concerted activity.

I find that Respondent’s Internet/Blogging policy is not unlawful under the *Lutheran Heritage Village* standard. The policy does not explicitly restrict Section 7 activity, and was not issued in response to an organizing campaign or other protected concerted activity. Furthermore, there is no evidence that Sanzone and Spinella were discharged pursuant to the policy or that the policy has otherwise been applied to restrict employees’ Section 7 rights. Therefore, the legality of the policy is contingent upon whether employees would reasonably construe it to prohibit Section 7 activity.

I find that under the existing case law, the Internet/Blogging policy would not be reasonably construed as prohibiting Section 7 activity.¹³ I find that the Internet/Blogging policy’s caution against “inappropriate discussions about the company, management, and/or co-workers” is similar to restrictions on speech having a potentially detrimental impact on the company which the Board has found to be permissible. See *Tradesmen International*, 338 NLRB 460, 462–463 (2002) (rule prohibiting “verbal or other statements which are slanderous or detrimental to the company or any of the company’s employees” permissible). The Board has similarly found that rules prohibiting any conduct, on or off-duty, which could injure the company’s reputation are not unlawful. *Tradesmen International*, 338 NLRB at 460 (prohibition on “any conduct which is disloyal, disruptive, competitive, or damaging to the company” permissible); *Ark Las Vegas Restaurant Corp.*, 335 NLRB 1284 fn. 2, 1291–1292 (2001) (rules prohibiting “any conduct, on or off duty, that tends to bring discredit to, or reflects adversely on, yourself, fellow associates, the Company,” and “conducting oneself unprofessionally or unethically, with the potential of damaging the reputation or a department of the

Company” not unlawful); *Flamingo Hilton-Laughlin*, 330 NLRB 287, 288–289 (1999) (rule prohibiting “off-duty misconduct that materially and adversely affects job performance or tends to bring discredit to the Hotel” did not violate Sec. 8(a)(1)); see also *Albertson’s, Inc.*, 351 NLRB 254, 258–259 (2007) (rule prohibiting “[o]ff the-job conduct which has a negative effect on the Company’s reputation or operation or employee morale or productivity”); *Lafayette Park Hotel*, 326 NLRB at 825–826 (rules prohibiting conduct which does not meet employer’s “goals and objectives,” and “improper conduct, which affects the employee’s relationship with the job, fellow employees, supervisors or the hotel’s reputation or good will in the community”).

This conclusion is supported by the context of the allegedly unlawful segment of the policy. The policy begins by stating that Respondent “supports the free exchange of information” among its employees, and states that only when electronic communications “extend to confidential and proprietary information” or “inappropriate discussions” would they potentially be subject to disciplinary action. Immediately following that statement is a requirement that employees clearly identify opinions they share regarding Respondent as their own, as opposed to those of Respondent. The policy closes by stating that it will have no effect to the extent it conflicts with State or Federal law. Under the case law discussed above, I find that in this context the prohibition on “inappropriate discussions about the company, management and/or co-workers” would not be reasonably construed as restricting Section 7 activity.

The General Counsel argues that the Internet/Blogging policy is impermissibly broad, in that it fails to provide specific examples of inappropriate discussions to clarify that it does not encompass protected activity. However, as the Board noted in *Tradesmen International*, the lawful rules at issue in *Lafayette Park Hotel*, *Ark Las Vegas Restaurant Corp.*, and *Flamingo Hilton-Laughlin* did not contain specific examples of conduct which would expose an employee to potential discipline for conduct injuring the employer’s reputation. *Tradesmen International*, 338 NLRB at 461; see *Lafayette Park Hotel*, 326 NLRB at 824–827; *Ark Las Vegas Restaurant Corp.*, 335 NLRB at 1291–1292; *Flamingo Hilton-Laughlin*, 330 NLRB at 287–288, 295. The General Counsel also argues that the policy here is similar to a policy the Board found unlawfully restrictive in *Claremont Resort & Spa*, 344 NLRB 832 (2005). In that case, the Board held that a policy which prohibited “negative conversations about associates and/or managers” could be reasonably construed as restricting Section 7 activity. *Claremont Resort & Spa*, 344 NLRB at 832. However, the facts at issue here are dissimilar. The prohibition on “negative conversations” in that case was issued to employees as part of a list of 10 work rules, some of which addressed working conditions such as “clocking in and out procedures,” so that the employees could assume that “negative conversations” regarding those conditions of employment were prohibited. *Claremont Resort & Spa*, 344 NLRB at 832 fn. 5. Here, by contrast, Respondent’s Internet/Blogging policy appears directed toward maintaining the company’s reputation with respect to the general public, as were the policies in the cases discussed above. Furthermore, the 10 work rules containing the unlawful restriction

¹³ Although Respondent contends that it did not in fact maintain the policy, the evidence establishes that when Respondent began its operations in December 2009 the policies contained in Respondent’s employee handbook were reviewed with Respondent’s initial group of employees, including Sanzone, at a meeting. DelBuono also offered to provide the employees at this meeting with copies of the handbook. Given the foregoing, I find that the policy was maintained by Respondent, despite the fact that Sanzone and Spinella never had their own physical copies of the handbook.

TRIPLE PLAY SPORTS BAR & GRILLE

on “negative conversations” were issued in the midst of an organizing campaign, and a previous administrative law judge’s decision had determined that the Respondent had unlawfully prohibited employees from discussing organizing activities while at work. *Claremont Resort & Spa*, 344 NLRB at 834, 836. As a result, I find that the facts at issue in *Claremont Resort & Spa* are distinguishable.

For all of the foregoing reasons, I find that Respondent’s maintenance of the Internet/Blogging policy in its employee handbook did not violate Section 8(a)(1) of the Act.

CONCLUSIONS OF LAW

1. The Respondent, Three D, LLC d/b/a Triple Play Sports Bar and Grille, is an employer engaged in commerce within the meaning of Section 2(6) and (7) of the Act.

2. Respondent violated Section 8(a)(1) of the Act by discharging Jillian Sanzone on February 2, 2011, in retaliation for her protected concerted activities.

3. Respondent violated Section 8(a)(1) of the Act by discharging Vincent Spinella on February 3, 2011, in retaliation for his protected concerted activities.

4. Respondent violated Section 8(a)(1) of the Act by threatening employees with legal action in retaliation for their protected concerted activities.

5. Respondent violated Section 8(a)(1) of the Act by informing employees that they were being discharged because of their protected concerted activities.

6. Respondent violated Section 8(a)(1) of the Act by threatening employees with discharge in retaliation for their protected concerted activities.

7. Respondent violated Section 8(a)(1) of the Act by coercively interrogating employees regarding their protected concerted activities.

8. Respondent did not violate Section 8(a)(1) of the Act by maintaining the Internet/Blogging policy in its employee handbook.

9. The above-described unfair labor practices affect commerce within the meaning of Section 2(2), (6), and (7) of the Act.

THE REMEDY

Having found that Respondent has violated the Act, I shall recommend that it cease and desist therefrom and take certain affirmative action necessary to effectuate the Act’s purposes.

Having discriminatorily discharged Jillian Sanzone and Vincent Spinella in retaliation for their protected concerted activities, Respondent must offer Sanzone and Spinella full reinstatement to their former positions or to substantially equivalent positions. Respondent must also make Sanzone and Spinella whole for any loss of earnings or other benefits they may have suffered as a result of the discrimination against them, plus interest, in the manner prescribed in *F. W. Woolworth*, 90 NLRB 289 (1950), and *New Horizons for the Retarded*, 283 NLRB 1173 (1987), compounded daily as prescribed in *Kentucky River Medical Center*, 356 NLRB No. 8 (2010). Respondent shall also be required to remove from its files all references to Sanzone and Spinella’s unlawful discharges, and to

notify them in writing that this has been done and that the discharges shall not be used against them.

On these findings of fact and conclusions of law and on the entire record, I issue the following recommended¹⁴

ORDER

The Respondent, Three D, LLC d/b/a Triple Play Sports Bar and Grille, Watertown, Connecticut, its officers, agents, successors, and assigns, shall

1. Cease and desist from

(a) Discharging or otherwise discriminating against employees because they engage in protected concerted activities.

(b) Threatening employees with legal action in retaliation for their protected concerted activities.

(c) Informing employees that they are being discharged because they engaged in protected concerted activities.

(d) Threatening employees with discharge in retaliation for their protected concerted activities.

(e) Coercively interrogating employees regarding their protected concerted activities.

(f) In any like or related manner interfering with, restraining, or coercing employees in the exercise of the rights guaranteed them by Section 7 of the Act.

2. Take the following affirmative action necessary to effectuate the policies of the Act.

(a) Within 14 days of the date of this Order, offer Jillian Sanzone and Vincent Spinella full reinstatement to their former positions or, if those positions no longer exists, to substantially equivalent positions, without prejudice to their seniority or to any other rights and privileges previously enjoyed.

(b) Make Jillian Sanzone and Vincent Spinella whole for any loss of earnings and other benefits suffered as a result of the discrimination against them, in the manner set forth in the remedy section of this decision.

(c) Within 14 days of the date of this Order, remove from all files any reference to the unlawful discharges, and within 3 days thereafter, notify Sanzone and Spinella in writing that this has been done and that the discharges will not be used against them in any way.

(d) Preserve and, within 14 days of a request, or such additional time as the Regional Director may allow for good cause shown, provide at a reasonable place designated by the Board or its agents, all payroll records, social security payment records, timecards, personnel records and reports, and all other records, including an electronic copy of such records if stored in electronic form, necessary to analyze the amount of backpay due under the terms of this Order.

(e) Within 14 days after service by the Region, post at its facility in Watertown, Connecticut, copies of the attached notice marked “Appendix.”¹⁵ Copies of the notice, on forms provided

¹⁴ If no exceptions are filed as provided by Sec. 102.46 of the Board’s Rules and Regulations, the findings, conclusions, and recommended Order shall, as provided in Sec. 102.48 of the Rules, be adopted by the Board and all objections to them shall be deemed waived for all purposes.

¹⁵ If this Order is enforced by a judgment of a United States court of appeals, the words in the notice reading “Posted by Order of the Na-

by the Regional Director for Region 34, after being signed by Respondent's authorized representative, shall be posted by the Respondent and maintained for 60 consecutive days in conspicuous places including all places where notices to employees are customarily posted. In addition to physical posting of paper notices, notices shall be distributed electronically, such as by e-mail, posting on an intranet or an internet site and/or other electronic means if Respondent customarily communicates with its employees by such means. Reasonable steps shall be taken by the Respondent to ensure that the notices are not altered, defaced, or covered by any other material. In the event that, during the pendency of these proceedings, the Respondent has gone out of business or closed the facility involved in these proceedings, the Respondent shall duplicate and mail, at its own expense, a copy of the notice to all current employees and former employees employed by the Respondent at any time since July 9, 2010.

(f) Within 21 days after service by the Region, file with the Regional Director a sworn certification of a responsible official on a form provided by the Region attesting to the steps that Respondent has taken to comply.

IT IS FURTHER ORDERED that the consolidated complaint is dismissed insofar as it alleges violations of the Act not specifically found.

APPENDIX

NOTICE TO EMPLOYEES

POSTED BY ORDER OF THE

NATIONAL LABOR RELATIONS BOARD

An Agency of the United States Government

The National Labor Relations Board has found that we violated Federal labor law and has ordered us to post and obey this notice.

tional Labor Relations board" shall read "Posted Pursuant to a Judgment of the United States Court of Appeals Enforcing an Order of the National Labor Relations Board."

FEDERAL LAW GIVES YOU THE RIGHT TO

- Form, join, or assist a union
- Choose representatives to bargain with us on your behalf
- Act together with other employees for your benefit and protection
- Choose not to engage in any of these protected activities.

WE WILL NOT discharge or otherwise discriminate against you because you engage in protected concerted activities.

WE WILL NOT threaten you with legal action in retaliation for your protected concerted activities.

WE WILL NOT inform you that you are being discharged because you engaged in protected concerted activities.

WE WILL NOT threaten you with discharge in retaliation for your protected concerted activities.

WE WILL NOT coercively interrogate you regarding your protected concerted activities.

WE WILL NOT in any like or related manner interfere with, restrain, or coerce you in the exercise of the rights guaranteed to you by Section 7 of the Act.

WE WILL, within 14 days of the date of the Board's Order, offer Jillian Sanzone and Vincent Spinella full reinstatement to their former jobs or, if those jobs no longer exist, to substantially equivalent positions, without prejudice to their seniority or any other rights and privileges previously enjoyed.

WE WILL make Jillian Sanzone and Vincent Spinella whole for any loss of earnings and other benefits suffered as a result of the discrimination against them, less any net interim earnings, plus interest.

WE WILL, within 14 days from the date of the Board's Order, remove from our files any reference to the unlawful discharges of Jillian Sanzone and Vincent Spinella, and WE WILL, within 3 days thereafter, notify Sanzone and Spinella in writing that this has been done and that the discharges will not be used against them in any way.

THREE D, LLC D/B/A TRIPLE PLAY SPORTS BAR AND GRILLE

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

SUMMARY ORDER

RULINGS BY SUMMARY ORDER DO NOT HAVE PRECEDENTIAL EFFECT. CITATION TO A SUMMARY ORDER FILED ON OR AFTER JANUARY 1, 2007, IS PERMITTED AND IS GOVERNED BY FEDERAL RULE OF APPELLATE PROCEDURE 32.1 AND THIS COURT'S LOCAL RULE 32.1.1. WHEN CITING A SUMMARY ORDER IN A DOCUMENT FILED WITH THIS COURT, A PARTY MUST CITE EITHER THE FEDERAL APPENDIX OR AN ELECTRONIC DATABASE (WITH THE NOTATION "SUMMARY ORDER"). A PARTY CITING A SUMMARY ORDER MUST SERVE A COPY OF IT ON ANY PARTY NOT REPRESENTED BY COUNSEL.

At a stated term of the United States Court of Appeals
for the Second Circuit, held at the Thurgood Marshall United
States Courthouse, 40 Foley Square, in the City of New York,
on the 23rd day of September, two thousand fourteen.

PRESENT: DENNIS JACOBS,
CHRISTOPHER F. DRONEY,
Circuit Judges
LEWIS A. KAPLAN,*
District Judge.

- - - - -X

LOIS TURNER,
Plaintiff-Appellant,

-v.-

13-3440-cv

TEMPTU INC., TEMPTU MARKETING INC.,
MICHAEL BENJAMIN,
Defendants-Appellees.

- - - - -X

* The Honorable Lewis A. Kaplan, of the United States District Court for the Southern District of New York, sitting by designation.

1 **FOR APPELLANT:**

DAVID G. EBERT (with Mioko C.
Tajika and Alissa G. Friedman on
the brief), Ingram Yuzek Gainen
Carroll & Bertolotti, LLP, New
York, New York.

7 **FOR APPELLEES:**

JUSTIN M. SHER, Sher Tremonte
LLP, New York, New York.

10 Appeal from a judgment of the United States District
11 Court for the Southern District of New York (Furman, J.).
12

13 **UPON DUE CONSIDERATION, IT IS HEREBY ORDERED, ADJUDGED**
14 **AND DECREED** that the judgment of the district court be
15 **AFFIRMED.**
16

17 Lois Turner appeals from the judgment of the United
18 States District Court for the Southern District of New York
19 (Furman, J.), granting summary judgment in favor of
20 defendants-appellees. We assume the parties' familiarity
21 with the underlying facts, the procedural history, and the
22 issues presented for review.
23

24 This action arises out of a failed business
25 relationship between Turner and defendants Temptu Inc.,
26 formerly known as Temptu Marketing Inc. ("Temptu"), and
27 Michael Benjamin (collectively, "Defendants"). Turner
28 alleges that after she entered into a partnership agreement
29 with them, Defendants stole her concept of a home-use
30 airbrush makeup system, thereby breaching the parties'
31 contract. Turner's complaint asserts eight causes of action
32 under New York law. On August 15, 2013, the district court
33 granted Defendants' motion for summary judgment and
34 dismissed all of Turner's claims. This appeal followed.¹
35

36 "We review the district court's grant of summary
37 judgment de novo, applying the same standards that govern
38 the district court's consideration of the motion." Summa v.
39 Hofstra Univ., 708 F.3d 115, 123 (2d Cir. 2013) (internal

¹ Turner does not appeal the dismissal of her claims
for breach of fiduciary duty, fraudulent inducement,
fraudulent concealment, and negligent misrepresentation.
Remaining are her causes of action for breach of contract
(express and implied), misappropriation of ideas, unjust
enrichment, and unfair competition.

1 quotation marks omitted). "The court shall grant summary
2 judgment if the movant shows that there is no genuine
3 dispute as to any material fact and the movant is entitled
4 to judgment as a matter of law." Fed. R. Civ. P. 56(a). A
5 fact is material if it "might affect the outcome of the suit
6 under the governing law." Anderson v. Liberty Lobby, Inc.,
7 477 U.S. 242, 248 (1986). A dispute concerning a material
8 fact is genuine "if the evidence is such that a reasonable
9 jury could return a verdict for the nonmoving party." Id.
10 On a motion for summary judgment, "[w]e resolve all
11 ambiguities and draw all reasonable inferences in the light
12 most favorable to the nonmoving party." Summa, 708 F.3d at
13 123.

14
15 A. Breach of Partnership / Joint Venture Agreement
16

17 Turner's first claim is that she and Benjamin "were
18 joint venturers by express and implied contract," and that
19 Benjamin breached the parties' agreement when he terminated
20 their partnership and marketed the airbrush system through
21 Temptu.² Compl. ¶¶ 45-47. Under New York law, the elements
22 of a cause of action for breach of contract are: (1) the
23 existence of a contract, (2) performance of the contract by
24 one party, (3) breach by the other party, and (4) damages
25 suffered as a result of the breach. Johnson v. Nextel
26 Commc'ns, Inc., 660 F.3d 131, 142 (2d Cir. 2011).
27

28 The requirements for a joint venture under New York law
29 include (1) that the parties' agreement "evidence their
30 intent to be joint venturers," (2) that each party "have
31 some degree of joint control over the venture," and (3) that
32 there be "a provision for the sharing of both profits and
33 losses." Dinaco, Inc. v. Time Warner, Inc., 346 F.3d 64,
34 67-68 (2d Cir. 2003) (quoting Itel Containers Int'l Corp. v.
35 Atlanttrafik Express Serv. Ltd., 909 F.2d 698, 701 (2d Cir.
36 1990)); see also Steinbeck v. Gerosa, 4 N.Y.2d 302, 151
37 N.E.2d 170, 178 (1958) ("An indispensable essential of a
38 contract of partnership or joint venture, both under common
39 law and statutory law, is a mutual promise or undertaking of

² Under New York law, "joint ventures are governed
by the same legal rules as partnerships because a joint
venture is essentially a partnership for a limited purpose."
Scholastic, Inc. v. Harris, 259 F.3d 73, 84 (2d Cir. 2001).
Accordingly, this summary order, like Turner's briefing,
will use both terms.

1 the parties to share in the profits of the business and
2 submit to the burden of making good the losses.").
3

4 Turner argues that a blog edited by herself, Benjamin,
5 and Roger Braimon constituted a binding joint venture
6 agreement. Turner testified that this blog--an "editable"
7 working document that was "constantly changing and
8 modifying," Turner Dep. at 93:4-94:11--contained the terms
9 of their oral partnership agreement and "served as a living
10 document for [them] to write, edit, and memorialize [their]
11 discussions." Turner Aff. ¶ 28. Having reviewed the
12 evidence in the light most favorable to Turner, we agree
13 with the district court that no rational juror could find
14 that Turner and Benjamin had finalized an agreement to which
15 they manifested an intent to be bound.
16

17 The key question whether a binding contract exists can
18 be answered only by looking to "the objective manifestations
19 of the intent of the parties as gathered by their expressed
20 words and deeds." Brown Bros. Elec. Contractors, Inc. v.
21 Beam Constr. Corp., 361 N.E.2d 999, 1001 (N.Y. 1977). "In
22 doing so, disproportionate emphasis is not to be put on any
23 single act, phrase or other expression, but, instead, on the
24 totality of all of these, given the attendant circumstances,
25 the situation of the parties, and the objectives they were
26 striving to attain." Id. at 1001.
27

28 Although the parties' blog contained a number of
29 possible contract terms, Turner admitted at her deposition
30 that many of these had not been finalized, see Turner Dep.
31 at 99:24-100:12, indeed, several of them were marked "to be
32 determined." Turner also acknowledged her understanding
33 that the alleged agreement was not finalized as late as
34 April 2007, when "still some discussion [] needed to take
35 place with respect to the contents of [their] contract."
36 Turner Dep. at 126:23-127:2; see also Turner Aff. Exs. 20,
37 21 (Turner stating that she could "bring a suggestion for a
38 contract/agreement" to the parties' meeting)). Also in
39 April, Braimon sent an e-mail to a lawyer, stating that the
40 parties had yet to "establish a contract" and were still
41 "undecided" even on the "actual product" they would develop
42 together. Sher Decl. Ex. 14. Perhaps most telling is that,
43 when asked at her deposition if the parties had ever
44 finalized their agreement, Turner responded, "No. I would
45 have loved to." Turner Dep. at 99:24-25. Given this
46 record, no reasonable jury could find that the parties

1 manifested the requisite intent to enter into a binding
2 partnership agreement.³
3

4 Accordingly, we affirm the dismissal of Plaintiff's
5 breach of contract claim.⁴
6

³ Defendants also argue (and the district court held) that there was no agreement to form a joint venture, because Turner, Benjamin, and Braimon never discussed--let alone agreed on--how the parties would share any losses. See Turner Dep. at 131:11-13 ("Did you ever discuss what would happen if the company lost money?" "No.")). There is some authority for Turner's proposition that courts will imply an equal division of losses where the parties have agreed to share equally in profits, see, e.g., Penato v. George, 383 N.Y.S. 2d 900, 904 (N.Y. App. Div. 2d Dep't 1976); but such cases "are inconsistent with more recent Appellate Division, Second Department authority," Mawere v. Landau, 39 Misc. 3d 1229(A), 1229A (N.Y. Sup. Ct. 2013) (collecting cases). Judicially implied loss sharing would seem to be particularly inappropriate where, as here, a plaintiff risks losing only the value of services she has invested while her putative partners stand to lose cash. Id. We decline to reach this issue, however, having found that the parties did not manifest a mutual assent to contract.

⁴ In the alternative, Turner argues that the parties' communications and conduct created an implied-in-fact contract. See Leibowitz v. Cornell Univ., 584 F.3d 487, 506-07 (2d Cir. 2009) (internal quotation marks and alterations omitted) ("Under New York law, a contract implied in fact may result as an inference from the facts and circumstances of the case, although not formally stated in words, and is derived from the presumed intention of the parties as indicated by their conduct."). Like any contract, an implied-in-fact contract "requires such elements as consideration, mutual assent, legal capacity and legal subject matter." Id. at 507. As explained above, the parties never finalized their agreement and never consented to its terms. Thus, no implied contract was formed. Id. at 507.

1 B. Misappropriation of Ideas

2
3 Next, Turner alleges that Defendants misappropriated
4 her idea to develop a new cosmetic airbrush system. "In
5 order for an idea to be susceptible to a claim of
6 misappropriation, two essential elements must be
7 established: the requisite legal relationship must exist
8 between the parties, and the idea must be novel and
9 concrete." McGhan v. Ebersol, 608 F. Supp. 277, 284
10 (S.D.N.Y. 1985) (citing Vantage Point, Inc. v. Parker Bros.,
11 Inc., 529 F. Supp. 1204, 1216 (E.D.N.Y.), aff'd without op.
12 sub. nom. Vantage Point, Inc. v. Milton Bradley, 697 F.2d
13 301 (2d Cir. 1982)). "The legal relationship between the
14 plaintiff and defendant may be either a fiduciary
15 relationship, or based on an express contract, an implied-
16 in-fact contract, or a quasi-contract." Id.

17
18 Turner argues that the legal relationship between her
19 and Benjamin is a contract or quasi-contract. As discussed
20 above, Turner fails to establish a contractual relationship;
21 and because the theory of quasi-contract is not distinct
22 from the theory of unjust enrichment, her quasi-contract
23 arguments fails for the reasons stated below. See Beth
24 Israel Med. Ctr. v. Horizon Blue Cross & Blue Shield of
25 N.J., Inc., 448 F.3d 573, 587 (2d Cir. 2006); Goldman v.
26 Metro. Life Ins. Co., 841 N.E.2d 742, 746 (N.Y. 2005).

27
28 Accordingly, we affirm the district court's dismissal
29 of this claim as well.

30
31 C. Unjust Enrichment & Unfair Competition

32
33 Plaintiff's claims for unjust enrichment and unfair
34 competition allege that Benjamin tricked her into working to
35 develop a novel airbrush system, only to steal it and take
36 the idea to Temptu, with which he was working all the while.

37
38 To establish unjust enrichment, a plaintiff must show
39 that the defendant was unjustly enriched at plaintiff's
40 expense and should in equity and good conscience return the
41 money. See In re First Cent. Fin. Corp., 377 F.3d 209, 213
42 (2d Cir. 2004); Bradkin v. Leverton, 257 N.E.2d 643 (N.Y.
43 1970). To sustain a claim for unfair competition, a
44 plaintiff must show that the defendant misappropriated the
45 plaintiff's labors or expenditures and that the defendant
46 displayed some element of bad faith in doing so. See, e.g.,

1 Jeffrey Milstein, Inc. v. Greger, Lawlor, Roth, Inc., 58
2 F.3d 27, 34-35 (2d Cir. 1995).
3

4 Both these claims fail. Temptu hired an independent
5 and highly trained engineer, Gennadi Fedorov, to develop and
6 design a new airbrush. There is no evidence that Fedorov
7 used any information or ideas from Turner, a graphic artist.
8 On the contrary, despite her awareness of Temptu's
9 application to patent the airbrush, Turner never objected.
10 The evidence demonstrates only that Turner and Benjamin
11 negotiated for a possible business venture that was never
12 formalized. That does not constitute unjust enrichment or
13 unfair competition. Accordingly, we affirm the dismissal of
14 these claims as well.
15

16 For the foregoing reasons, and finding no merit in
17 Turner's other arguments, we hereby **AFFIRM** the judgment of
18 the district court.
19

20 FOR THE COURT:
21 CATHERINE O'HAGAN WOLFE, CLERK
22
23
24
25

FOR PUBLICATION

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

JANE DOE NO. 14,
Plaintiff-Appellant,

v.

INTERNET BRANDS, INC.,
DBA Modelmayhem.com,
Defendant-Appellee.

No. 12-56638

D.C. No.
2:12-cv-03626-
JFW-PJW

OPINION

Appeal from the United States District Court
for the Central District of California
John F. Walter, District Judge, Presiding

Argued and Submitted
February 7, 2014—Pasadena, California

Filed September 17, 2014

Before: Mary M. Schroeder and Richard R. Clifton, Circuit
Judges, and Brian M. Cogan, District Judge.*

Opinion by Judge Clifton

* The Honorable Brian M. Cogan, District Judge for the U.S. District Court for the Eastern District of New York, sitting by designation.

SUMMARY**

Communications Decency Act

The panel reversed the district court's Federal Rule Civil Procedure 12(b)(6) dismissal of a diversity action alleging negligence under California law, and concluded that the claim was not barred by the federal Communications Decency Act.

The Jane Doe plaintiff alleged that Internet Brands, Inc.'s failure to warn users of its networking website, modelmayhem.com, caused her to be a victim of a rape scheme. Section 230(c)(1) of the Communications Decency Act precludes liability that treats a website as the publisher or speaker of information users provide on the website, and generally protects websites from liability for material posted on the website by someone else.

The panel held that Doe's negligent failure to warn claim did not seek to hold Internet Brands liable as the "publisher or speaker of any information provided by another information content provider," and therefore the Communications Decency Act did not bar the claim. The panel expressed no opinion on the viability of the failure to warn allegations on the merits, and remanded for further proceedings.

** This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

COUNSEL

Jeffrey Herman (argued) and Stuart S. Mermelstein, Herman Law, Boca Raton, Florida, for Plaintiff-Appellant.

Patrick Fraioli, Ervin Cohen & Jessup LLP, Beverly Hills, California; Wendy E. Giberti (argued), iGeneral Counsel, P.C., Beverly Hills, California, for Defendant-Appellee.

OPINION

CLIFTON, Circuit Judge:

Model Mayhem is a networking website, found at modelmayhem.com, for people in the modeling industry. Plaintiff Jane Doe, an aspiring model who posted information about herself on the website, alleges that two rapists used the website to lure her to a fake audition, where they drugged her, raped her, and recorded her for a pornographic video. She also alleges that Defendant Internet Brands, the company that owns the website, knew about the rapists but did not warn her or the website's other users. She filed an action against Internet Brands alleging liability for negligence under California law based on that failure to warn.

The district court dismissed the action on the ground that her claim was barred by the Communications Decency Act ("CDA"), 47 U.S.C. § 230(c) (2012). We conclude that the CDA does not bar the claim. We reverse and remand for further proceedings.

I. Background

At the motion to dismiss stage, we assume factual allegations stated in the Complaint filed by Plaintiff to be true.¹ *Sprewell v. Golden State Warriors*, 266 F.3d 979, 988 (9th Cir. 2001). Plaintiff alleges that Internet Brands owns and operates the website modelmayhem.com, which it purchased in 2008. Model Mayhem is a networking site for professional and aspiring models to market their services. It has over 600,000 members. Plaintiff Jane Doe, a fictitious name, was an aspiring model who became a member of Model Mayhem.

Unbeknownst to Jane Doe, two persons, Lavont Flanders and Emerson Callum, were using Model Mayhem to identify targets for a rape scheme, allegedly as early as 2006. Flanders and Callum are not alleged to have posted their own profiles on the website. Instead, they browsed profiles on Model Mayhem posted by models, contacted potential victims with fake identities posing as talent scouts, and lured the victims to south Florida for modeling auditions. Once a victim arrived, Flanders and Callum used a date rape drug to put her in a semi-catatonic state, raped her, and recorded the activity on videotape for sale and distribution as pornography.

In 2008, Internet Brands purchased Model Mayhem from Donald and Taylor Waitts, the original developers of the site. Shortly after the purchase, Internet Brands learned of how Flanders and Callum were using the website. In August 2010, Internet Brands sued the Waitts for failing to disclose the

¹ Given the serious nature of the allegations, we note that Internet Brands has specifically denied substantially all of the allegations, including that the assailants contacted Plaintiff through the website.

potential for civil suits arising from the activities of Flanders and Callum. By that time, according to Jane Doe, Internet Brands knew that Flanders and Callum had used Model Mayhem to lure multiple women to the Miami area to rape them.

In February 2011, Flanders, pretending to be a talent scout, contacted Jane Doe, in the words of the Complaint, “through Model Mayhem.” Jane Doe went to south Florida for a purported audition, where Flanders and Callum drugged, raped, and recorded her.

Jane Doe filed this diversity action against Internet Brands in the Central District of California, where Internet Brands is based, asserting one count of negligent failure to warn under California law. She alleges that Internet Brands knew about the activities of Flanders and Callum but failed to warn Model Mayhem users that they were at risk of being victimized. She further alleges that this failure to warn caused her to be a victim of the rape scheme.

Internet Brands filed a motion to dismiss the action under Federal Rule of Civil Procedure 12(b)(6), on the ground that her claim was barred by the CDA. The district court granted the motion to dismiss and dismissed the action with prejudice. It denied leave to amend the complaint on the ground that any amendment would be futile. Jane Doe appeals.

II. Discussion

We review de novo a district court’s decision to grant a motion to dismiss. *Edwards v. Marin Park, Inc.*, 356 F.3d 1058, 1061 (9th Cir. 2004). We also review de novo

questions of statutory interpretation. *United States v. Harvey*, 659 F.3d 1272, 1274 (9th Cir. 2011).

California law imposes a duty to warn a potential victim of third party harm when a person has a “special relationship to either the person whose conduct needs to be controlled or . . . to the foreseeable victim of that conduct.” *Tarasoff v. Regents of Univ. of California*, 17 Cal.3d 425, 435 (1976), *superseded by statute*, Cal. Civ. Code § 43.92. Jane Doe alleges that Internet Brands had a cognizable “special relationship” with her and that its failure to warn her of Flanders and Callum’s rape scheme caused her to fall victim to it. Internet Brands argues that the CDA precludes the claim. Although we assume that Internet Brands may contest the scope of the duty to warn under California law and, in particular, the existence of the required special relationship, that issue is not before us. The dismissal of the action by the district court was based entirely on the CDA.

The question before us, therefore, is whether the CDA bars Jane Doe’s negligent failure to warn claim under California law. We begin with the language of the statute. *Campbell v. Allied Van Lines Inc.*, 410 F.3d 618, 620 (9th Cir. 2005).

Sections 230(c)(1) and (2) of the CDA provide:

(c) Protection for “Good Samaritan” blocking and screening of offensive material

(1) Treatment of publisher or speaker

No provider or user of an interactive computer service shall be treated as the

publisher or speaker of any information provided by another information content provider.

(2) Civil liability

No provider or user of an interactive computer service shall be held liable on account of—

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

An “information content provider” is, under section 230(f)(3), “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.” Thus, section 230(c)(1) precludes liability that treats a website as the publisher or speaker of information users provide on the website. In general, this

section protects websites from liability for material posted on the website by someone else.

Under section 230(c)(1), the protection applies even though the website proprietor has not acted to remove offensive content posted by others. For example, this court has held that the CDA barred a negligent undertaking claim against a website that failed to remove an offensive profile posted on the website by the victim's ex-boyfriend. *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1101–03 (9th Cir. 2009). Such liability, the court explained, would “treat” the website as the “publisher” of user content because “removing content is something publishers do” and to permit liability for such conduct “necessarily involves treating the liable party as a publisher of the content it failed to remove.” *Id.* at 1103.

Jane Doe's claim is different, however. She does not seek to hold Internet Brands liable as a “publisher or speaker” of content someone posted on the Model Mayhem website, or for Internet Brands' failure to remove content posted on the website. Flanders and Callum are not alleged to have posted anything themselves. The Complaint alleges only that “JANE DOE was contacted by Lavont Flanders through MODEL MAYHEM.COM using a fake identity.” Jane Doe also does not claim to have been lured by any posting that Internet Brands failed to remove.

Instead, Jane Doe attempts to hold Internet Brands liable for failing to warn her about how third parties targeted and lured victims through Model Mayhem. The duty to warn allegedly imposed by California law would not require Internet Brands to remove any user content or otherwise affect how it publishes such content. Any obligation to warn could have been satisfied without changes to the content

posted by the website's users. Internet Brands would simply have been required to give a warning to Model Mayhem users, perhaps by posting a notice on the website or by informing users by email what it knew about the activities of Flanders and Callum.

Posting or emailing such a warning could be deemed an act of publishing information, but section 230(c)(1) bars only liability that treats a website as a publisher or speaker of content provided by somebody else: in the words of the statute, "information provided by another information content provider." 47 U.S.C. § 230(c)(1). A post or email warning that Internet Brands generated would involve only content that Internet Brands itself produced. An alleged tort based on a duty that would require such a self-produced warning therefore falls outside of section 230(c)(1). In sum, Jane Doe's negligent failure to warn claim does not seek to hold Internet Brands liable as the "publisher or speaker of any information provided by another information content provider." *Id.* As a result, we conclude that the CDA does not bar this claim.

The core policy of section 230(c)(1) supports this conclusion. As the heading to section 230(c) indicates, the purpose of that section is to provide "[p]rotection for 'Good Samaritan' blocking and screening of offensive material." That means a website should be able to act as a "Good Samaritan" to self-regulate offensive third party content without fear of liability. In particular, section 230 was in part a reaction to *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995) (unpublished), a New York state court decision holding that an internet service provider became a "publisher" of offensive content on its message boards because it deleted some

offensive posts but not others. *Id.* at *4. Under *Stratton Oakmont*'s reasoning, a website had to choose between voluntarily removing some offensive third party content, which would expose the site to liability for the content it did not remove, or filtering nothing, which would prevent liability for all third party content. *See id.* "In passing section 230, Congress sought to spare interactive computer services this grim choice by allowing them to perform some editing on user-generated content without thereby becoming liable for all defamatory or otherwise unlawful messages that they didn't edit or delete." *Fair Housing Council v. Roommates.Com, LLC*, 521 F.3d 1157, 1163 (9th Cir. 2008).

Jane Doe's failure to warn claim has nothing to do with Internet Brands' efforts, or lack thereof, to edit or remove user generated content. The theory is that Internet Brands should be held liable, based on its knowledge of the rape scheme and its "special relationship" with users like Jane Doe, for failing to generate its own warning. Liability would not discourage "Good Samaritan" filtering of third party content. The core policy of section 230(c), reflected in the statute's heading, does not apply, and neither does the CDA's bar.

Another policy of section 230 is to "avoid the chilling effect upon Internet free speech that would be occasioned by the imposition of tort liability upon companies that do not create potentially harmful messages but are simply intermediaries for their delivery." *Delfino v. Agilent Techs., Inc.*, 52 Cal. Rptr. 3d 376, 387 (Ct. App. 2006). As section 230(b) itself explains, "[i]t is the policy of the United States . . . to promote the continued development of the Internet . . . [and] to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive

computer services, unfettered by Federal or State regulation.” Broadly speaking, Internet Brands was an “intermediary” between Jane Doe and the rapists, but there is no allegation that Model Mayhem transmitted any potentially harmful messages between Jane Doe and Flanders or Callum. There is also no allegation that Flanders or Callum posted their own profiles on the website.

In any case, that Internet Brands was in some sense an “intermediary” between Jane Doe and the rapists does not mean that the failure to warn claim treats Internet Brands as the publisher or speaker of user content. True, imposing any tort liability on Internet Brands for its role as an interactive computer service could be said to have a “chilling effect” on the internet, if only because such liability would make operating an internet business marginally more expensive. But such a broad policy argument does not persuade us that the CDA should bar the failure to warn claim. We have already held that the CDA does not declare “a general immunity from liability deriving from third-party content.” *Barnes*, 570 F.3d at 1100. Congress has not provided an all purpose get-out-of-jail-free card for businesses that publish user content on the internet, though any claims might have a marginal chilling effect on internet publishing businesses. Moreover, the argument that our holding will have a chilling effect presupposes that Jane Doe has alleged a viable failure to warn claim under California law. That question is not before us and remains to be answered.

Barring Jane Doe’s failure to warn claim would stretch the CDA beyond its narrow language and its purpose. To be sure, Internet Brands acted as the “publisher or speaker” of user content by hosting Jane Doe’s user profile on the Model Mayhem website, and that action could be described as a

“but-for” cause of her injuries. Without it, Flanders and Callum would not have identified her and been able to lure her to their trap. That does not mean the failure to warn claim seeks to hold Internet Brands liable as the “publisher or speaker” of user content, however. Publishing activity is a but-for cause of just about everything Model Mayhem is involved in. It is an internet publishing business. Without publishing user content, it would not exist. As noted above, however, we held in *Barnes* that the CDA does not provide a general immunity against all claims derived from third-party content. In that case we affirmed the dismissal of a claim for negligent undertaking as barred under the CDA, as discussed above at 8, but we reversed the dismissal of a claim for promissory estoppel under Oregon law. The publication of the offensive profile posted by the plaintiff’s former boyfriend was a “but-for” cause there, as well, because without that posting the plaintiff would not have suffered any injury. But that did not mean that the CDA immunized the proprietor of website from all potential liability.

The parties discuss other court decisions regarding the CDA in their briefs. The case law provides no close analogies, though, because the cases are all distinguishable in critical respects. The key factors discussed in prior cases are not present here. The purported tort duty does not arise from allegations about mishandling the removal of third party content. *Barnes*, 570 F.3d at 1105–06 (holding that the CDA bars negligent undertaking claim arising from Yahoo’s failure to take reasonable care in removing offensive profiles). Nor is there a contractual duty arising from a promise distinct from tort duty arising from publishing conduct. *Id.* at 1108–09 (holding that the CDA does not bar a promissory estoppel claim). The tort duty asserted here does not arise from an alleged failure to adequately regulate access to user

content. *Doe II v. MySpace, Inc.*, 175 Cal.App.4th 561, 573 (Ct. App. 2009) (holding that the CDA bars tort claims based on a duty to restrict access to minors' MySpace profiles). There is in our case no employer-employee relationship giving rise to a negligent supervision claim. *Lansing v. Southwest Airlines Co.*, 980 N.E.2d 630, 639–41 (Ill. Ct. App. 2012) (holding that the CDA does not bar a negligent supervision claim against an airline whose employee used the company email and text messaging systems to harass the plaintiff). In short, this case presents the novel issue of whether the CDA bars Jane Doe's failure to warn claim under California law. We conclude that it does not.

III. Conclusion

The CDA does not bar Jane Doe's failure to warn claim. We express no opinion on the viability of the failure to warn allegations on the merits. We hold only that the CDA is not a valid basis to dismiss Jane Doe's complaint. Accordingly, we reverse and remand for proceedings consistent with this opinion.

REVERSED AND REMANDED.

1
2
3
4
5
6 UNITED STATES DISTRICT COURT
7 FOR THE NORTHERN DISTRICT OF CALIFORNIA
8 OAKLAND DIVISION

9
10 SUNBELT RENTALS, INC.,

11 Plaintiff,

12 vs.

13 SANTIAGO VICTOR,

14 Defendant.

Case No: C 13-4240 SBA

**ORDER GRANTING PLAINTIFF'S
MOTION TO DISMISS
DEFENDANT'S
COUNTERCLAIMS**

Dkt. 39

15
16 Sunbelt Rentals, Inc. ("Plaintiff" or "Sunbelt") filed the instant action against its
17 former employee, Santiago Victor ("Defendant" or "Victor"), alleging that he
18 misappropriated trade secrets upon his termination. Victor has filed five counterclaims
19 against Sunbelt, accusing it, inter alia, of violating the federal Wiretap Act and the Stored
20 Communications Act ("SCA") by reviewing his text messages on the iPhone which Sunbelt
21 had previously issued to him. The parties are presently before the Court on Plaintiff's
22 Motion to Dismiss Defendants Counterclaims. Having read and considered the papers filed
23 in connection with this matter and being fully informed, the Court hereby GRANTS the
24 motion and dismisses Victor's counterclaims, with leave to amend. The Court, in its
25 discretion, finds this matter suitable for resolution without oral argument. Fed. R. Civ. P.
26 78(b); N.D. Cal. Civ. L.R. 7-1(b).

1 **I. BACKGROUND**

2 **A. RELEVANT FACTS**

3 During the relevant time period, Victor worked as an outside sales representative for
4 Sunbelt, an equipment rental company. Countercl. ¶ 11, Dkt. 34. In August 2013, Victor
5 gave his two-week notice to Sunbelt, stating that he had taken a job with one of its
6 competitors—Ahern Rentals (“Ahern”). Id. ¶ 16. Upon learning of Victor’s intent to leave
7 the company, Sunbelt immediately dismissed him. Id.

8 During his time with Sunbelt, Victor was assigned a Sunbelt-owned iPhone
9 (“Sunbelt iPhone”) and a Sunbelt-owned iPad for both work and personal purposes. Id.
10 ¶¶ 12-14. Thereafter, Victor “created and paid for a personal ‘Apple account’ that was
11 linked to both devices.” Id. ¶ 15. Victor returned the devices to Sunbelt after his
12 separation. Id. ¶¶ 16, 18, 20.

13 Victor’s new employer, Ahern, provided him a new iPhone (“Ahern iPhone”). Id.
14 ¶¶ 19-20. At some point thereafter, Victor registered or linked his Ahern iPhone to the same
15 personal Apple account he had previously used while at Sunbelt. Id. ¶ 19. This process
16 “synced” Victor’s Ahern iPhone with his personal Apple account. Id.

17 Several weeks later, when he received a new iPad from Ahern (“Ahern iPad”),
18 Victor linked the new iPad to his personal Apple account. Id. ¶ 20. In the process of
19 registering the Ahern iPad, Victor discovered the telephone number associated with the
20 Sunbelt iPhone was still linked to his personal Apple account. Id. Because Victor had
21 failed to unlink the Sunbelt iPhone from his account, his “private electronic data and
22 electronic messages,” including text messages sent to and from his Ahern iPhone, also were
23 transmitted to the Sunbelt iPhone which he had returned to Sunbelt. Id. ¶ 20, 21. Victor
24 then deleted the Sunbelt number from his account “to ensure that his new Ahern issued
25 Apple products were not in any way linked to Sunbelt.” Id.

26 Victor claims that after his departure, Sunbelt “began actively investigating Victor’s
27 post-employment acts, conduct, and communications.” Id. ¶ 21. In the course of such
28 investigation, Sunbelt allegedly “invaded Victor’s privacy rights by *accessing*,

1 *intercepting, monitoring, reviewing, storing and using* Victor’s post-employment private
2 electronic data and electronic communications (including but not limited to *text messages*
3 sent and received from Victor’s Ahern, Rentals Inc. issued iPhone) without authority,
4 permission, or consent.” *Id.* (emphasis added). Victor further accuses Sunbelt of
5 “*intentionally accessing* Victor’s private electronic communications and data, without
6 authorization, from facilities through which Victor’s electronic communications were
7 provided and stored (i.e., Victor’s cellular phone provider’s network which stores Victor’s
8 electronic communications, and or Apple’s cloud based network where Victor’s electronic
9 communication pertaining to his Apple Account are processed and stored) and where such
10 services and communications were restricted to access by Victor, which Sunbelt obtained
11 through improper means.” *Id.* ¶ 23 (emphasis added). No particular facts are alleged to
12 support these assertions.

13 **B. PROCEDURAL HISTORY**

14 On September 12, 2013, Sunbelt filed a complaint against Victor in this Court
15 alleging four state law causes of action: (1) breach of contract; (2) misappropriation of trade
16 secrets; (3) unfair competition; and (4) breach of duty of loyalty. Dkt. 1. Victor then filed
17 an Answer, and later amended an Answer and Counterclaim. The gist of the Counterclaim
18 is that Sunbelt improperly read the text messages that were inadvertently transmitted to his
19 Sunbelt iPhone. He alleges claims for violations of: (1) the Wiretap Act; (2) the SCA; (3)
20 California Penal Code § 502 et seq.; (4) California Penal Code § 630 et seq.; and (5) his
21 right to privacy. *See* Countercl. ¶ 24. Each of these claims is based on the same set of
22 facts—Sunbelt’s purported interception, acquisition and use of Victor’s electronic
23 communications (i.e., text messages) sent to and from his Ahern iPhone. Sunbelt now
24 moves to dismiss all counterclaims. This matter has been fully briefed and is ripe for
25 adjudication.

26 **II. LEGAL STANDARD**

27 Pleadings in federal court actions are governed by Federal Rule of Civil Procedure
28 8(a)(2), which requires only “a short and plain statement of the claim showing that the

pleader is entitled to relief.” Rule 12(b)(6) “tests the legal sufficiency of a claim.” Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). A complaint may be dismissed under Rule 12(b)(6) for either failure to state a cognizable legal theory or insufficient facts to support a cognizable legal theory. Mendiondo v. Centinela Hosp. Med. Ctr., 521 F.3d 1097, 1104 (9th Cir. 2008). “[C]ourts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice.” Tellabs, Inc. v. Makor Issues & Rights, Ltd., 551 U.S. 308, 322 (2007). The court is to “accept all factual allegations in the complaint as true and construe the pleadings in the light most favorable to the nonmoving party.” Outdoor Media Group, Inc. v. City of Beaumont, 506 F.3d 895, 899-900 (9th Cir. 2007).

To survive a motion to dismiss, “a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). The complaint must afford the defendants with “fair notice” of the claims against them, and the grounds upon which the claims are based. Swierkiewicz v. Sorema N.A., 534 U.S. 506, 512 (2002). “Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” Iqbal, 556 U.S. at 678. When a complaint or claim is dismissed, “[l]eave to amend should be granted unless the district court determines that the pleading could not possibly be cured by the allegation of other facts.” Knappenberger v. City of Phoenix, 566 F.3d 936, 942 (9th Cir. 2009).

III. DISCUSSION

A. WIRETAP ACT

The Wiretap Act imposes civil liability against any person who “*intentionally intercepts*, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C §§ 2511(1)(a) (emphasis added); id. § 2520(a). The Act defines “intercept” as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic,

1 mechanical, or other device.” 18 U.S.C. § 2510(4). “Such acquisition occurs ‘when the
2 contents of a wire communication are captured or redirected in any way.’” Noel v. Hall,
3 568 F.3d 743, 749 (9th Cir. 2009). The inception must be intentional, as opposed to
4 inadvertent. See Sanders v. Robert Bosch Corp., 38 F.3d 736, 742-43 (4th Cir. 1994).

5 Here, Victor has failed to allege facts sufficient to establish that Sunbelt
6 “intentionally intercepted” any of his text messages. By Victor’s own account, the text
7 messages appeared on his Sunbelt iPhone as a result of Victor’s act of syncing his new
8 iPhone to his Apple account without first un-linking his Sunbelt iPhone. Countercl. ¶¶ 19,
9 20. In other words, Sunbelt did not intentionally capture or redirect Victor’s text messages
10 to the Sunbelt iPhone—the transmission of those messages was entirely Victor’s doing.
11 Given these circumstances, the requisite intentional conduct is lacking. Sanders, 38 F.3d at
12 742-43; Shubert v. Metrophone, Inc., 898 F.2d 401, 405 (3rd Cir. 1990) (noting that
13 Congress specifically intended that “inadvertent interceptions are not crimes under [the
14 Wiretap Act]”).

15 Nor has Victor alleged facts sufficient to establish that Sunbelt acted to “intercept”
16 the text messages or any other electronic communications. The Ninth Circuit applies a
17 “narrow definition of ‘intercept.’” Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878
18 (9th Cir. 2002). For a communication to be intercepted, “it must be acquired during
19 transmission, not while it is in electronic storage.” Id. Though Victor vaguely alleges that
20 Sunbelt intercepted his electronic communications, i.e., his text messages, he provides no
21 facts to support this otherwise conclusory assertion.¹ If anything, the pleadings suggest that
22 Sunbelt read Victor’s text messages *after* they were sent and received on the Sunbelt
23 iPhone, which is insufficient to demonstrate intentional interception under the Wiretap Act.
24 See NovelPoster v. Javitch Canfield Group, No. C 13-5186 WHO, 2014 WL 3845148, *10
25 (N.D. Cal. Aug. 14, 2014) (reading emails that have already been received in an email

26
27 ¹ Victor’s Counterclaim repeatedly makes vague and formulaic references to
28 “private and electronic communications,” but only specifically identifies “text messages” as
having been allegedly intercepted. See Countercl. ¶ 22. Victor never specifies how the
alleged interception transpired.

1 account's inbox does not constitute interception under the Wiretap Act because the
2 transmission had already occurred).

3 Although it is clear that Victor's Wiretap Act claim must be dismissed, what is less
4 clear is whether leave to amend should be granted. Given the almost instantaneous
5 transmission of text messages, the window during which an interception may occur is
6 exceedingly narrow. NovelPoster, 2014 WL 3845148, *10 (citing United States v. Steiger,
7 318 F.3d 1039, 1050 (11th Cir. 2003)). Thus, "unless some type of automatic routing
8 software is used" to divert the text message, interception of [a text message] within the
9 prohibition of the Wiretap Act is virtually impossible." Id. (internal quotations and citation
10 omitted). Given these constraints, it is doubtful that Victor will be able to allege facts,
11 consistent with Federal Rule of Civil Procedure 11, to state a claim for violation of the
12 Wiretap Act. Nonetheless, the Court will afford Victor an opportunity to amend this claim
13 and therefore DISMISSES his claim under the Wiretap Act, with leave to amend.²

14 **B. STORED COMMUNICATIONS ACT**

15 The SCA creates "a cause of action against anyone who "intentionally accesses
16 without authorization a facility through which an electronic communication service is
17 provided . . . and thereby obtains, alters, or prevents authorized access to a wire or
18 electronic communication while it is in electronic storage.'" Theofel v. Farey-Jones, 359
19 F.3d 1066, 1072 (9th Cir. 2004) (quoting 18 U.S.C. §§ 2701(a)(1), 2707(a)). "[E]lectronic
20 storage" is defined as either "temporary, intermediate storage . . . incidental to . . .
21 electronic transmission," or "storage . . . for purposes of backup protection." 28 U.S.C.
22 § 2510(17).

23 According to Victor, Sunbelt violated the SCA by virtue of having,

24 Intentionally accessed, without authorization, facilities through
25 which Victor's electronic communications were provided and
26 stored (i.e., Victor's cellular phone provider's network which
stores Victor's electronic communications, and or Apple's

27 ² Sunbelt also contends that Victor has failed to allege any facts showing that it
28 intercepted his text messages "through the use of any . . . device." 18 U.S.C. § 2510(4)
(emphasis added). Since it is clear that the Counterclaim fails to allege intentional
interception, the Court need not reach that issue at this juncture.

cloud based network where Victor's electronic communication pertaining to his Apple Account are processed and stored) and where such services and communications were restricted to access by Victor, which Sunbelt obtained through improper means.

Countercl. ¶ 45. No facts are presented, however, to support the conclusory assertion that Sunbelt *accessed* Victor's text messages through his cellular telephone provider or Apple's network. Moreover, in his opposition, Victor contradicts himself by stating that the text messages allegedly accessed by Sunbelt "were *not* accessed through, nor stored on a website." Opp'n at 4 (emphasis added). To the extent that Victor is claiming that Sunbelt accessed his text messages by reviewing the messages on his Sunbelt iPhone—as he does elsewhere in his Counterclaim, such conduct does not violate the SCA. See Garcia v. City of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012) (holding that text messages and pictures stored on a cellular telephone do not constitute "electronic storage" for purposes of the SCA). This claim is DISMISSED with leave to amend.

C. CALIFORNIA PENAL CODE § 502

Section 502 of the California Penal Code prohibits unauthorized access to computers, computer systems, and computer networks, and provides for a civil remedy in the form of compensatory damages, injunctive relief, and other equitable relief. Cal. Penal Code § 502. Section 502 is an anti-hacking statute intended to prohibit the unauthorized use of any computer system for improper or illegitimate purpose. Yee v. Lin, No. C 12-02474 WHA, 2012 WL 4343778, *2 (N.D. Cal. Sept. 20, 2012).

Victor alleges that Sunbelt violated subsections (c)(1), (2), (3), (4), (6), and (7) of Section 502, which provides that a person is liable if he:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

...

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

Id. § 502(c); Countercl. ¶ 54. For purposes of Section 502, parties act "without permission" when they "circumvent[] technical or code-based barriers in place to restrict or bar a user's access." Facebook, Inc. v. Power Ventures, Inc., 844 F. Supp. 2d 1025, 1036 (N.D. Cal. 2012).

In his third Counterclaim, Victor alleges as follows:

On information and belief, Sunbelt violated California Penal Code section 502 when it improperly began accessing, intercepting, monitoring, reviewing and using Victor's post-employment private electronic data and electronic communications without Victor's knowledge, authorization or consent. On information and belief, Sunbelt additionally, or in the alternative, violated of Penal Code § 502 ***by intentionally accessing, without authorization***, facilities through which Victor's electronic communications were provided and stored (i.e., Victor's cellular phone provider's network which stores Victor's electronic communications, and or Apple's cloud based network where Victor's electronic communication pertaining to his Apple Account are processed and stored) and where such services and communications were restricted to access by Victor, which Sunbelt obtained through improper means.

Countercl. ¶ 56 (emphasis added). These fact-barren and vague allegations are precisely the type of "threadbare recitals" proscribed by Twombly and Iqbal. Moreover, to the extent that Victor is claiming that Sunbelt accessed his unspecified "private electronic data and electronic communications" through the Apple account or his cellular telephone provider's computer network, such a claim fails on the ground that no facts are alleged showing that Sunbelt did so by circumventing technical or code-based barriers intended to restrict such

1 access. Facebook, 844 F. Supp. 2d at 1036. To the contrary, Victor simply avers that
2 Sunbelt reviewed his text messages that he caused, albeit inadvertently, to be sent to the
3 Sunbelt iPhone. The Court therefore concludes that Victor has failed to state a claim under
4 Section 502 and DISMISSES said claim with leave to amend.

5 **D. CALIFORNIA PENAL CODE § 630**

6 The California Invasion of Privacy Act (“CIPA”) is intended to prevent privacy
7 invasions facilitated by modern technology and devices. Cal. Penal Code § 630. “The
8 analysis for a violation of CIPA is the same as that under the federal Wiretap Act.”
9 NovelPoster, 2014 WL 3845148, *12 (granting judgment on pleadings on CIPA claim for
10 same reasons underlying the dismissal of the plaintiff’s Wiretap Act claim, i.e., the lack of
11 intentional interception). As discussed, Victor has failed to plausibly allege a violation of
12 the Wiretap Act; *a fortiori*, he is also unable to allege a violation of CIPA. This claim is
13 DISMISSED with leave to amend.

14 **E. INVASION OF PRIVACY**

15 California recognizes four categories of the tort of invasion of privacy: (1) intrusion
16 upon seclusion; (2) public disclosure of private facts; (3) false light in the public eye; and
17 (4) appropriation of name or likeness. Shulman v. Group W Prods., Inc., 18 Cal.4th 200,
18 214 n. 4 (1998). Victor fails to indicate which type of invasion of privacy claim he is
19 alleging. Nonetheless, based on the sparse allegations presented, it appears that he is
20 attempting to state a claim for intrusion upon seclusion.

21 “A privacy violation based on the common law tort of intrusion has two elements.
22 First, the defendant must intentionally intrude into a place, conversation, or matter as to
23 which the plaintiff has a reasonable expectation of privacy. Second, the intrusion must
24 occur in a manner highly offensive to a reasonable person.” Hernandez v. Hillsides, Inc.,
25 47 Cal.4th 272, 285 (2009). “The tort is proven only if the plaintiff had an objectively
26 reasonable expectation of seclusion or solitude in the place, conversation or data source.”
27 Shulman v. Grp. W Prods., Inc., 18 Cal.4th 200, 232 (1998). A plaintiff pursuing an
28 invasion of privacy action must have conducted himself or herself in a manner consistent

1 with an actual expectation of privacy, i.e., he or she must not have engaged in conduct
2 which manifests a voluntary consent to the invasive actions of defendant. Hill v. Nat'l
3 Collegiate Athletic Ass'n, 7 Cal.4th 1, 26 (1994).

4 Victor contends that, as a matter of law, an employee has a reasonable expectation of
5 privacy with respect to text messages contained on employer-owned mobile telephones.
6 The decisional authorities cited by Victor, however, are inapposite. In City of Ontario v.
7 Quon, 560 U.S. 746 (2010), a police officer was issued a pager by his police department
8 which was subject to a limit on the number of characters that could be sent and received
9 each month. Id. at 750. After becoming concerned that the officer was repeatedly
10 exceeding his character limit, the police department obtained transcripts of the text
11 messages from the wireless carrier to ascertain whether the texts were work-related or
12 personal. Id. at 750-51. After finding that most of the text messages were not work-
13 related, the police department took disciplinary action against the officer. Id. at 753. The
14 police officer then brought an action under 42 U.S.C. § 1983 against the city, police
15 department and police chief, alleging that the police department's review of his text
16 messages violated the Fourth Amendment.

17 In the addressing the plaintiff's Fourth Amendment claim, the United States
18 Supreme Court *assumed, without deciding*, that the plaintiff had a reasonable expectation
19 of privacy in text messages sent to him on an employer-provided pager; however, the Court
20 ultimately upheld the police department's review of those messages as reasonable under the
21 Fourth Amendment. Id. at 760. Despite Victor's suggestion to the contrary, the Supreme
22 Court did not hold that an employee automatically has an expectation of privacy in
23 electronic messages stored on a device provided by his employer. Quon also is
24 distinguishable on its facts. Unlike the police officer in Quon, Victor was no longer an
25 employee of the company that owned the electronic device at issue at the time the invasion
26 of privacy allegedly occurred. Moreover, unlike the police department, which requested
27 transcripts of the text messages from the wireless carrier, Sunbelt is not alleged to have
28 affirmatively undertaken any action to obtain and review the text messages or any other

1 electronic data. Rather, the electronic communications appeared on Sunbelt's iPhone
2 because of actions taken by Victor.

3 Victor's citation to United States v. Finley, 477 F.3d 250 (5th Cir. 2007) fares no
4 better. In that case, a criminal defendant challenged the denial of his motion to suppress
5 text messages and call records which law enforcement officials had obtained through a
6 warrantless search of his employer-issued cell phone. In addressing the threshold issue of
7 whether the defendant had standing to raise a Fourth Amendment challenge, the Fifth
8 Circuit held that the mere fact that the employer owned the phone and had access to its
9 contents did not ipso facto demonstrate that defendant correspondingly had no expectation
10 of privacy in his call records and text messages. Id. at 259. In reaching its decision, the
11 court specifically noted that the defendant had undertaken precautions to maintain the
12 privacy of data stored on his phone and that he "had a right to exclude others from using the
13 phone." Id. Unlike the defendant in Finley, Victor was no longer an employee of the
14 company which owned the cell phone to which the subject text messages had been sent. In
15 addition, Victor had no right to exclude others from accessing the Sunbelt iPhone—which
16 he did not own or possess and no longer had any right to access. Moreover, rather than
17 undertake precautions to maintain the privacy of his text messages, Victor did just the
18 opposite by failing to unlink his Sunbelt iPhone from his Apple account, which, in turn,
19 facilitated the transmission of those messages to an iPhone exclusively owned, controlled
20 and possessed by his former employer.

21 Victor's privacy claim also fails on the ground that he has failed to show an
22 intrusion into a "place, conversation, or matter as to which the plaintiff has a reasonable
23 expectation of privacy." Hernandez, 47 Cal.4th at 285. As noted, Victor cannot
24 legitimately claim an expectation of privacy in a "place," i.e., the Sunbelt iPhone, which
25 belongs to his former employer and to which he has no right to access. Nor can Victor
26 claim a reasonable expectation of privacy with respect to his text messages, in general. The
27 pleadings do not identify the contents of any particular text messages, and instead, refer
28 generally to "private electronic data and electronic communications." Countercl. ¶ 79.

1 This and other courts have concluded that there is no “legally protected privacy interest and
2 reasonable expectation of privacy” in electronic messages, “in general.” In re Yahoo Mail
3 Litig., -- F. Supp. 2d --, 2014 WL 3962824, *16 (N.D. Cal. Aug. 12, 2014) (citing cases).³
4 Rather, a privacy interest can exist, if at all, only with respect to the *content* of those
5 communications. In any event, even if Victor were claiming an expectation of privacy with
6 respect to the specific content of his text messages (which he has not specified), the facts
7 alleged demonstrate that he failed to comport himself in a manner consistent with an
8 objectively reasonable expectation of privacy. By his own admission, Victor personally
9 caused the transmission of his text messages to the *Sunbelt* iPhone by syncing his new
10 devices to his Apple account without first unlinking his Sunbelt iPhone.⁴ As such, even if
11 he *subjectively* harbored an expectation of privacy in his text messages, such expectation
12 cannot be characterized as *objectively* reasonable, since it was *Victor’s* conduct that directly
13 caused the transmission of his text messages to Sunbelt in the first instance. See Hill,
14 7 Cal.4th at 26.

15 The above notwithstanding, the facts alleged in Victor’s fifth counterclaim are
16 insufficient to show that Sunbelt intruded into Victor’s privacy in a manner highly
17 offensive to a reasonable person. “Actionable invasions of privacy must be sufficiently
18 serious in their nature, scope, and actual or potential impact to constitute an egregious
19 breach of the social norms underlying the privacy right.” Hill, 7 Cal. 4th at 37. In addition,
20 the plaintiff must show “that the *use* of plaintiff’s information was highly offensive.”
21 Folgelstrom v. Lamps Plus, Inc., 195 Cal. App. 4th 986, 993 (2011) (emphasis added)
22 (upholding the demurrer to plaintiff’s common law invasion of privacy claim where,
23

24 ³ Victor also does not specify whether his claim is predicated upon text messages
25 sent by him, received by him, or both. With respect to messages he transmitted, there is
26 authority finding that a plaintiff has no reasonable expectation of privacy in messages sent
27 to third parties. See Fetsch v. City of Roseburg, No. 6:11-cv-6343-TC, 2012 WL 6742665,
*10 *(D.Or. Dec. 31, 2012) (plaintiff had no expectation of privacy in text messages sent
from his phone because relinquished control of them once they were transmitted).

28 ⁴ Victor vaguely alleges that Sunbelt intercepted his electronic communications. He
provides no factual support for this conclusory assertion. See Countercl. ¶ 77.

1 finding that even if the customer addresses were obtained through “questionable” means,
2 there was “no allegation that Lamps Plus used the address once obtained for an offensive or
3 improper purpose.”).

4 Here, Victor alleges only that Sunbelt acted in a “highly offensive” manner by
5 “accessing, intercepting, monitoring, reviewing, storing and using [his] post-employment
6 private electronic data and electronic communications without [his] knowledge,
7 authorization or consent as part of an unreasonably intrusive and unauthorized investigation
8 into Victor’s post-employment conduct.” Countercl. ¶ 79. Victor offers no factual support
9 for these conclusory assertions. In particular, he provides no details regarding the specific
10 conduct by Sunbelt that amounts to “accessing, intercepting, monitoring, reviewing, storing
11 and using [his] post-employment private electronic data and electronic communications.”

12 Id. He also fails to aver any facts to establish that Sunbelt’s use of the intercepted
13 communications was highly offensive. See Folgelstrom, 195 Cal. App. 4th at 993. The
14 possibility that Sunbelt may have reviewed text messages sent to a cell phone which it
15 owned and controlled—without more—is insufficient to establish an offensive use. As
16 with his other claims, Victor’s formulaic recitation of an invasion of privacy claim is
17 inconsistent with the federal pleading requirements of Rule 8. This claim is DISMISSED
18 with leave to amend.

19 **IV. CONCLUSION**

20 For the reasons stated above,

21 IT IS HEREBY ORDERED THAT:

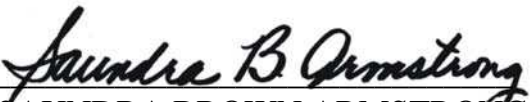
22 1. Plaintiff’s Motion to Dismiss Defendants Counterclaims is GRANTED.

23 2. Defendant shall have twenty-one (21) days from the date this Order is filed to
24 amend his counterclaims, consistent with the Court’s rulings. Defendant is warned that any
25 factual allegations set forth in his amended pleading must be made in good faith and
26 consistent with Rule 11. The failure to timely file the amended counterclaim and/or the
27 failure to comply with this Order will result in the dismissal of all counterclaims with
28 prejudice.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

IT IS SO ORDERED.

Dated: August 28, 2014


SAUNDRA BROWN ARMSTRONG
United States District Judge

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
ANNABELLE ZARATZIAN,

Plaintiff,

v.

ADEL RAMSEY ABADIR and

LARRY M. CARLIN,

Defendants.
-----X

MEMORANDUM DECISION

10 CV 9049 (VB)

Briccetti, J.:

Plaintiff Annabelle Zaratzian commenced this action against defendants Adel Ramsey Abadir and Larry M. Carlin on December 3, 2010, asserting violations of 18 U.S.C. § 2510 et seq. (the “Wiretap Act”), 18 U.S.C. § 2701 et seq. (the “Stored Communications Act” or “SCA”), and for conspiracy to violate those Acts under 42 U.S.C. § 1985(3), as well as state law claims for violation of New York Penal Law § 250.05 and trespass to chattels.

On January 31, 2011, Abadir and Carlin moved to dismiss the complaint under Rule 12(b)(6). (Docs. ##12, 14). On May 3, 2011, the Honorable J. Frederick Motz, sitting by designation, denied Abadir’s motion, but granted Carlin’s motion, holding Zaratzian had not plausibly pleaded any claims as against Carlin. (Doc. #21).

Zaratzian appealed Judge Motz’s decision to the Court of Appeals for the Second Circuit,¹ which granted her motion to stay the appeal because final judgment had not yet been entered. This Court granted Zaratzian’s motion for entry of final judgment pursuant to Rule 54(b) as to the dismissed defendant, Carlin, and directed the Clerk to enter judgment as to Carlin. (Doc. #34). The Court of Appeals lifted the stay.

¹ On June 21, 2011, Zaratzian filed an amended complaint naming Abadir as the sole defendant. (Doc. #30-1).

On February 10, 2012, while her appeal was pending, Zaratzian moved under Rule 62.1 for an indicative ruling on her motion under Rule 60(b)(2) seeking relief from the final Judgment entered as to Carlin on the basis of newly discovered evidence. (Doc. #65).

By Memorandum Decision dated May 30, 2012, the Court granted Zaratzian's motion for an indicative ruling, and stated it would grant Zaratzian's motion to re-open the case against Carlin if the Court of Appeals were to remand for that purpose. (Doc. #62). On August 14, 2012, the Court of Appeals did remand the case to this Court. (Doc. #76). Accordingly, Zaratzian moved for relief from the Judgment dismissing all claims against Carlin pursuant to Rule 60(b)(2), which the Court granted on August 29, 2012, thereby reinstating Carlin as a defendant. (Doc. #78).

Zaratzian thereafter filed a second amended complaint ("SAC"). (Doc. #80). The SAC asserts federal claims against both defendants under the Wiretap Act and the Stored Communications Act and state law claims against Abadir for trespass to chattels, constructive fraud by fiduciary, and violation of New York Penal Law § 250.05. Zaratzian also seeks injunctive relief under Section 2520(b) of the Wiretap Act and Section 2707(b) of the SCA.

Now pending are Abadir's and Carlin's motions for summary judgment² and Zaratzian's motion for partial summary judgment. (Docs. ##110, 114, and 118).

The Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1367.

² Although his motion for summary judgment seeks dismissal of the SAC in its entirety, Abadir does not make any arguments specifically addressing Zaratzian's state law claims for trespass to chattels and violation of New York Penal Law § 250.05.

In addition to the arguments Carlin advances in his own motion for summary judgment, he also "fully adopt[s]" those asserted by Abadir. (See Doc. #116 at 5).

BACKGROUND

The parties have submitted briefs, statements of facts pursuant to Local Civil Rule 56.1, and exhibits, which reflect the following factual background.

Zaratzian and Abadir married in 1993, separated in 2005, and, following contentious matrimonial litigation, divorced in 2006. In connection with their divorce, Zaratzian and Abadir entered into a “marital separation agreement,” dated December 19, 2006. (Doc. #126-1). The post-divorce period was acrimonious, including litigation in the Westchester County Family Court regarding child custody and related issues.

On August 30, 2001—while the couple was still married—Abadir opened a Cablevision “Optimum Online” account for internet and email service. Because Zaratzian was unfamiliar with computers, on April 10, 2003, Abadir configured an email account for Zaratzian (azaratzian@optonline.net) and set her password. Abadir thus had access to Zaratzian’s email messages and her account settings, including an email-forwarding setting which, if enabled, automatically forwards all incoming email to a designated email address.

Abadir enabled the “auto-forwarding” function at some point before the couple’s separation in September 2005, causing all incoming emails sent to Zaratzian at azaratzian@optonline.net to be automatically forwarded to Abadir at his email address, rabadir@optonline.net. Abadir testified that when he activated the auto-forwarding function, he told Zaratzian he was doing so to avoid missing notifications about their children’s extracurricular activities, and that Zaratzian agreed to it. Zaratzian denies this. Abadir maintains he discussed the function with Zaratzian at the time he enabled it, but agrees there were no subsequent conversations about it. When Abadir was asked at his deposition if emails forwarded from Zaratzian’s account to his account included electronic communications with third parties, including Zaratzian’s attorneys, he conceded they did.

Sometime after the couple separated, Zaratzian took over the Cablevision account, and the name associated with the account was changed from Abadir's to Zaratzian's on November 14, 2005. (See Doc. #111-5). Several years later, on June 4, 2009, Zaratzian called Cablevision and, upon learning Abadir's email account was still being maintained, instructed Cablevision to close Abadir's account. The account was deactivated that day. Abadir thus received copies of Zaratzian's incoming emails until Zaratzian instructed Cablevision to close Abadir's email account on June 4, 2009.

Because Abadir's account was no longer active, Zaratzian began receiving error messages stating "Delivery Notification: Delivery has failed." She dismissed these messages as "spam" until she examined a series of them on June 27, 2010, and observed the error messages related to Abadir's email address. Zaratzian again contacted Cablevision and learned her email account had been set to automatically forward her incoming emails to rabadir@optonline.net.

One of the emails automatically forwarded to Abadir was a June 3, 2009, email from Zaratzian's accountant with Zaratzian's 2008 federal and state income tax returns attached. On May 18, 2010, Abadir sent his divorce attorney, defendant Larry M. Carlin, an email with Zaratzian's 2008 tax returns attached. The email's subject line was "Annabelle 2008 RETURN & AUTHORIZATION FORM," and the body of the email contained the message "Enclosed are materials that may be useful. Ramsey." (Doc. #116-1).

In October 2010, during a Family Court proceeding relating to the parties' respective finances, Carlin claimed Zaratzian earned \$400,000 per year. Zaratzian argues this statement was based on information gleaned from her 2008 tax returns, which Abadir surreptitiously acquired in June 2009 via the email auto-forwarding function.

Carlin testified he only learned Abadir had been receiving copies of Zaratzian's emails in December 2010 when he was served with Zaratzian's original complaint in this action. Zaratzian contends she has submitted evidence of other incidents showing Carlin knew or had reason to know about the auto-forwarding.

DISCUSSION

I. Legal Standard

The Court must grant a motion for summary judgment if the pleadings, discovery materials before the Court, and any affidavits show there is no genuine issue as to any material fact and it is clear the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986).

A fact is material when it "might affect the outcome of the suit under the governing law. . . . Factual disputes that are irrelevant or unnecessary" are not material and thus cannot preclude summary judgment. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986).

A dispute about a material fact is genuine if there is sufficient evidence upon which a reasonable jury could return a verdict for the non-moving party. See id. The Court "is not to resolve disputed issues of fact but to assess whether there are any factual issues to be tried." Wilson v. Nw. Mut. Ins. Co., 625 F.3d 54, 60 (2d Cir. 2010) (citation omitted). It is the moving party's burden to establish the absence of any genuine issue of material fact. Zalaski v. City of Bridgeport Police Dep't, 613 F.3d 336, 340 (2d Cir. 2010).

If the non-moving party has failed to make a sufficient showing on an essential element of his case on which he has the burden of proof, then summary judgment is appropriate. Celotex Corp. v. Catrett, 477 U.S. at 323. If the non-moving party submits "merely colorable" evidence, summary judgment may be granted. Anderson v. Liberty Lobby, Inc., 477 U.S. at 249-50. The

non-moving party “must do more than simply show that there is some metaphysical doubt as to the material facts, and may not rely on conclusory allegations or unsubstantiated speculation.” Brown v. Eli Lilly & Co., 654 F.3d 347, 358 (2d Cir. 2011) (internal citations omitted). The mere existence of a scintilla of evidence in support of the non-moving party’s position is likewise insufficient; there must be evidence on which the jury could reasonably find for him. Dawson v. Cnty. of Westchester, 373 F.3d 265, 272 (2d Cir. 2004).

In deciding a summary judgment motion, the Court construes the facts, resolves all ambiguities, and draws all permissible factual inferences in favor of the non-moving party. Dallas Aerospace, Inc. v. CIS Air Corp., 352 F.3d 775, 780 (2d Cir. 2003). If there is any evidence from which a reasonable inference could be drawn in favor of the non-moving party on the issue on which summary judgment is sought, summary judgment is improper. See Sec. Ins. Co. of Hartford v. Old Dominion Freight Line Inc., 391 F.3d 77, 83 (2d Cir. 2004).

II. Statutes of Limitations

Defendants argue Zaratzian’s Wiretap Act and Stored Communications Act claims, brought on December 3, 2010, are barred by the statutes of limitations in those Acts.

Under the Wiretap Act, a civil action “may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.” 18 U.S.C. § 2520(e). “In other words, the [Wiretap Act] bars a suit if the plaintiff had such notice as would lead a reasonable person either to sue or to launch an investigation that would likely uncover the requisite facts.” Sparshott v. Feld Entm’t, Inc., 311 F.3d 425, 429 (D.C. Cir. 2002); accord Lanier v. Bryant, 332 F.3d 999, 1004 (6th Cir. 2003). Actual knowledge of the violation is not required. Davis v. Zirkelbach, 149 F.3d 614, 618 (7th Cir. 1998) (Section

2520(e) “does not require the claimant to have actual knowledge of the violation; it demands only that the claimant have had a reasonable opportunity to discover it.”).

Likewise, “[a] civil action under [the SCA] may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.” 18 U.S.C. § 2707(f); see also Maddalena v. Toole, 2013 WL 5491869, at *4 (C.D. Cal. Oct. 1, 2013) (holding the limitations provision of the SCA “do[es] not require that the claimant have actual knowledge of the violation . . . only . . . reasonable notice”).

Defendants have the burden to show the absence of a genuine issue of fact as to the untimeliness of Zaratzian’s claims. See Lanier v. Bryant, 332 F.3d at 1003 (citing Celotex Corp. v. Catrett, 477 U.S. at 323); see also Sweeten v. Middle Twp., 2007 WL 4440936, at *7 (D.N.J. Dec. 14, 2007) (“Where a defendant raises a section 2520(e) defense in the context of a summary judgment motion, it bears the burden of establishing that ‘no reasonable jury could [find that the plaintiff] did not have a reasonable opportunity to discover [the violation] more than two years before the start of the lawsuit.’” (quoting Sparshott v. Feld Entm’t, Inc., 311 F.3d at 429)).

Here, defendants argue two “red flags” put Zaratzian on notice of the alleged violation. First, in a November 11, 2007 email, Abadir told Zaratzian: “At my last count the kids have been exposed to 3 of your significant others in the last several months.” (Doc. #111-6). Defendants contend this put Zaratzian on notice that Abadir was intercepting her emails, because Zaratzian knew her children had not met (and did not know) the men she had dated, and because Zaratzian had only communicated the fact that she dated three men over email. Second, in the summer or fall of 2008, Zaratzian and Abadir’s daughter relayed to Zaratzian a conversation in which Abadir used a distinctive phrase (“ADD loser idiot”) to describe Zaratzian’s then-boyfriend

Harold Burke. Defendants urge this, too, put Zaratzian on notice because in early 2008, Burke forwarded to Zaratzian an email from Burke's ex-wife describing Burke with the same phrase.

Zaratzian concedes these communications occurred but contends the significance of the communications at the time is in dispute.

The Court cannot, as a matter of law, conclude that these two incidents would alert a reasonable person to the alleged violation. Accordingly, whether and when Zaratzian had a reasonable opportunity to discover the violation is a question of fact for the jury. See, e.g., Brown v. Am. Broad. Co., Inc., 704 F.2d 1296, 1304 (4th Cir. 1983) (holding in Wiretap Act case that "the issue of when plaintiff knew, or reasonably should have known of the existence of her cause of action, is a question to be resolved by a jury").

Defendants also argue Zaratzian's testimony that she suspected Abadir was reading her emails more than two years before she commenced this action shows Zaratzian had inquiry notice of the alleged violations. Zaratzian's testimony about her own suspicions is irrelevant, however, as the standard is objective. See Sparshott v. Feld Entm't, Inc., 311 F.3d at 429 ("[The plaintiff's] subjective state of mind is irrelevant.").³ The question is whether, objectively, the two incidents submitted by defendants gave Zaratzian the kind of notice that "would lead a reasonable person either to sue or to launch an investigation that would likely uncover the requisite facts." Id. The Court concludes this is in dispute.

Accordingly, defendants' motions for summary judgment on the Wiretap Act and SCA claims based on the statutes of limitations are denied.

³ Moreover, Zaratzian's testimony is not nearly as clear on this point as defendants suggest. For example, Zaratzian also testified she "didn't understand how [Abadir] knew all these little things about me that he shouldn't have known," and she also had speculated her neighbors might be spying on and/or watching her. (Doc. #111-1 at 33-34). Zaratzian further testified that it was only "in hindsight"—that is, with the benefit of more information—that these incidents led her to conclude Abadir was reading her email. (Id. at p. 34).

III. The Wiretap Act

Zaratzian asserts claims against Abadir and Carlin under the Wiretap Act. “Through the enactment of [the Electronic Communications Privacy Act (“ECPA”)], Congress amended the Federal wiretap law in order to ‘update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.’” Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 (2d Cir. 2005) (quoting Sen. Rep. No. 99–541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555).⁴ Subject to certain exceptions, anyone who “intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication” has violated the Wiretap Act. 18 U.S.C. § 2511(1)(a); see also id. § 2520 (providing private right of action).

Zaratzian asserts claims against Abadir for intercepting her email communications under Section 2511(1)(a), and for disclosing and using the contents of the allegedly intercepted communications under Sections 2511(1)(c) and 2511(1)(d), respectively. Under the Wiretap Act, it is also unlawful intentionally to disclose or use, or endeavor to disclose or use, “the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [Section 2511].” 18 U.S.C. §§ 2511(1)(c), 2511(1)(d).

Zaratzian also asserts claims against Carlin for disclosing and using the contents of the allegedly intercepted communications under Sections 2511(1)(c) and 2511(1)(d).

⁴ “ECPA is divided into Title I, which governs unauthorized interception of electronic communications, 18 U.S.C. §§ 2510-2522 [the Wiretap Act], and Title II, which governs unauthorized access to stored communications, 18 U.S.C. §§ 2701-2711 [the Stored Communications Act].” Id.

A. Interception

Defendants argue Zaratzian’s Wiretap Act claims should be dismissed because the automatic forwarding of emails does not constitute an interception under the Act.

“Intercept” is defined by the Act as “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4). “[E]lectronic communication means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” *Id.* § 2510(12) (internal quotation marks omitted).

Although no such requirement appears explicitly in the Act, several circuit courts of appeals have concluded on the basis of statutory interpretation and legislative history that an interception of an electronic communication must be “contemporaneous” with the transmission of the communication to violate Section 2511. See Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 110, 113-14 (3d Cir. 2003) (employer’s search of employee’s email stored on central file server not interception because not contemporaneous with transmission); United States v. Steiger, 318 F.3d 1039, 1047-50 (11th Cir. 2003) (use of “Trojan Horse” computer virus “to access and download information stored on [a] personal computer” not interception because not contemporaneous with transmission); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878-79 (9th Cir. 2002) (access of secure website not interception because not contemporaneous with transmission); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460-62 (5th Cir. 1994) (“seizure of a computer on which is stored private [e]mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients” not interception because not contemporaneous with transmission).

At least two courts in this District have adopted this “narrow” definition of “intercept.” Snyder v. Fantasy Interactive, Inc., 2012 WL 569185, at *2 (S.D.N.Y. Feb. 9, 2012) (“While the Second Circuit has not addressed this issue, the Fifth Circuit’s reason for maintaining the narrow definition is sound, and this Court adopts it.” (internal citations omitted)); Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417, 430 (S.D.N.Y. 2010) (order on summary judgment); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 557-58 (S.D.N.Y. 2008) (order on motion to preclude use of emails as evidence).

Assuming, without deciding, that an interception must be contemporaneous with the communication to violate the Wiretap Act, the Court concludes the interception at issue here—the auto-forwarding of emails received by Zaratzian’s email account to Abadir’s email account—satisfies that standard.

In United States v. Szymuszkiewicz, the Seventh Circuit addressed substantially the same issue before the Court—whether a Microsoft Outlook rule “that directed Outlook to forward to [the defendant] all messages [his supervisor] received” was a contemporaneous interception under the Wiretap Act. 622 F.3d 701, 703 (7th Cir. 2010). The Seventh Circuit held it was contemporaneous, rejecting the defendant’s attempt to analogize an individual intercepting electronic communications to a football player “catching a thing in flight,” id. at 705-06—the same analogy offered by defendants here. The Seventh Circuit held the defendant’s analogy was inapt because “contemporaneous” does not mean “in the middle,” and “for email there is no single ‘thing’ that flies straight from sender to recipient.” Id. Rather, “[t]here are only packets, segments of a message that take different routes at different times.” Id. at 705. The court reasoned:

Either the server in Kansas City or [the defendant’s supervisor’s] computer made copies of the messages for [the defendant] within a

second of each message's arrival and assembly; if both [the defendant] and [the defendant's supervisor] were sitting at their computers at the same time, they would have received each message with no more than an eyeblink in between. That's contemporaneous by any standard. Even if [the defendant's supervisor's] computer (rather than the server) was doing the duplication and forwarding, it was effectively acting as just another router, sending packets along to their destination.

Id. at 706 (emphasis added).

The Court agrees with the Seventh Circuit's commonsense application of the contemporaneity requirement in a case with materially identical facts. Here, too, whether it was the server or Zaratzian's computer that made the copies that were transmitted to Abadir,⁵ those copies were made "within a second of each message's arrival and assembly," and if both Zaratzian and Abadir were at their computers in the same moment, they each would have received the message "with no more than an eyeblink in between." Id.; see also Doc. #136 (Abadir's Resp. to Pl.'s Statement of Undisputed Facts) ¶¶ 72-75. The Court therefore concludes the automatic forwarding in question constitutes a contemporaneous interception of electronic communications under the Wiretap Act.⁶

Defendants contend the Second Circuit has cited Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994), and the cases following it "with approval, thereby endorsing the prevailing line of cases differentiating electronic communications 'in transit' (and therefore subject to interception under the Wiretap Act) from those 'in storage' (which are not)." (Doc. #113 at 31 n.8 (citing Hall v. EarthLink Network, Inc., 396 F.3d 500 (2d Cir. 2005))).

⁵ It appears to be undisputed that the copying was done by an application called a "mail transfer agent" on the Optimum Online server.

⁶ Defendants characterize Szymuszkiewicz as the "minority view." In Szymuszkiewicz, however, the Seventh Circuit did not reject the contemporaneity rule advanced by the other circuit courts of appeals. It held the automatic forwarding of emails at issue was contemporaneous. United States v. Szymuszkiewicz, 622 F.3d at 705-06. Therefore, it does not represent a "minority view." In any event, defendants make no attempt to distinguish its facts.

First, the Court rejects defendants’ reading of the dicta in Hall, a case involving the continued receipt and storage of email messages by EarthLink (an internet service provider) after EarthLink terminated the plaintiff’s account. In Hall, the Second Circuit disposed of EarthLink’s alternative arguments—specifically, that “communication over the Internet can only be electronic communication while it is in transit, not while it is in electronic storage,” and “an ‘interception’ can only occur when messages are in transit.” Hall v. EarthLink Network, Inc., 396 F.3d at 503 n.1. Without explicitly addressing the merits of the Steve Jackson Games cases, the Second Circuit distinguished them, thereby rejecting EarthLink’s alternative arguments and concluding that unlike those cases, the case before it involved “the continued receipt of e-mail messages rather than the acquisition of previously stored electronic communication.” Id.⁷

Second, if anything, the dicta in Hall undermines defendants’ position, as the interception here strikes the Court as more similar to the “continued receipt of e-mail messages” in Hall than “the acquisition of previously stored electronic communication” in the Steve Jackson Games cases. See id. at 503 n.1; see also Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 556 (S.D.N.Y. 2008) (observing the Second Circuit in Hall “was unpersuaded by the defendant’s argument that an interception . . . can only occur when messages are in transit, but did not elaborate further.” (internal quotation marks omitted)).

In any event, because the automatic email forwarding here was contemporaneous with communication, it constitutes interception even under the so-called “narrow” standard applied in the Steve Jackson Games cases.⁸

⁷ The Second Circuit went on to hold that an exception for electronic communications intercepted in the “ordinary course of business” applied, thus concluding on the basis of that exception that EarthLink’s receipt of emails did not constitute an interception. Id. at 504-05.

⁸ Defendants urge the Court to apply the “rule of lenity,” a canon of statutory interpretation, to resolve “any remaining ambiguity” in their favor. “The rule of lenity is a rule of

Accordingly, Zaratzian's partial motion for summary judgment is granted on the narrow issue of whether an interception of an electronic communication occurred. See 18 U.S.C. §§ 2510(4), 2510(12), and 2511(1)(a).⁹

B. Consent

Defendants further argue Zaratzian consented to the interception of her email by "allow[ing] her husband to establish her e-mail account and set her password, . . . thus grant[ing] him wholesale authorization to access her account as he saw fit." (Doc. #113 at 20).

Under the Wiretap Act, an interception of an electronic communication is not unlawful when "one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). "Such consent may be express or implied." United States v. Willoughby, 860 F.2d 15, 19 (2d Cir. 1988). "[I]mplied consent is 'consent in fact[,] which is inferred 'from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance.'" Griggs-Ryan v. Smith, 904 F.2d 112, 116-17 (1st Cir. 1990) (quoting United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)); see also Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) ("Without actual notice, consent can only be implied when "[t]he surrounding circumstances . . . convincingly show that the party knew about and consented to the interception."). "[T]he parameters of consent may be circumscribed depending on the subtleties and permutations inherent in a particular set of facts[, and] a reviewing court must inquire into the dimensions of

last resort, [applied] only when none of the other canons of statutory interpretation is capable of resolving the statute's meaning." Adams v. Holder, 692 F.3d 91, 107 (2d Cir. 2012) (internal quotation marks omitted). Because the meaning of the applicable provisions of the Wiretap Act are capable of being resolved, the rule of lenity is not applicable. See id. Regardless, even assuming arguendo, as the Court has, that the "narrow" definition of interception applied in the Steve Jackson Games cases is correct, the automatic email forwarding here nevertheless constitutes interception for the reasons stated above.

⁹ This ruling has no effect on the Court's determinations that issues of fact remain regarding (i) whether and when Zaratzian had a reasonable opportunity to discover the interception, and (ii) the scope of Zaratzian's implied consent to the interception (see infra).

the consent and then ascertain whether the interception exceeded those boundaries.” Griggs-Ryan v. Smith, 904 F.2d at 119. Defendants bear the burden of demonstrating the consent exception applies. See In re Pharmatrak, Inc., 329 F.3d 9, 19 (1st Cir. 2003).

It is not genuinely disputed that Zaratzian permitted Abadir to open an Optimum Online email account for her, configure that account, and set her initial password.¹⁰ Zaratzian does, however, dispute the scope of that initial consent.

The Court agrees with Zaratzian that the scope of her consent is an issue of fact. See, e.g., In re Pharmatrak, Inc., 329 F.3d at 19 (“A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications.”); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581-82 (11th Cir. 1983) (“[K]nowledge of the capability of monitoring alone cannot be considered implied consent. . . . It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent.”); In re Google Inc. Gmail Litig., 2014 WL 1102660, at *16 (N.D. Cal. Mar. 18, 2014) (“Implied consent is an intensely factual question that requires consideration of the circumstances surrounding the interception to divine whether the party whose communication was intercepted was on notice that the communication would be intercepted.”).

The issue is not whether Zaratzian ever impliedly “revoked” her consent, as defendants assert, but, rather, the scope of Zaratzian’s consent and whether the interception here exceeded

¹⁰ In Zaratzian’s Response to Abadir’s Statement of Undisputed Facts, Zaratzian denies Abadir “had access to a password utilized by her” and states she does not recall whether Abadir came up with the first password on her email account or a subsequent password, citing her affidavit. (Doc. #127 at 2). Zaratzian testified at her deposition, however, that Abadir “came up with” her initial password, and Zaratzian, on summary judgment, may not undermine that deposition testimony with an affidavit. Hayes v. N.Y.C. Dep’t of Corr., 84 F.3d 614, 619 (2d Cir. 1996) (“[A] party may not create an issue of fact by submitting an affidavit in opposition to a summary judgment motion that, by omission or addition, contradicts the affiant’s previous deposition testimony.”). The Court therefore treats this fact as undisputed for purposes of these motions.

that consent. The Court is not persuaded the permission Zaratzian gave Abadir to set up her email account and choose a password for her constitutes “wholesale” consent to Abadir reading her personal emails in perpetuity, as a matter of law. Therefore, defendants have not shown the absence of a genuine issue of material fact regarding Zaratzian’s consent to the interception. See Zalaski v. City of Bridgeport Police Dep’t, 613 F.3d 336, 340 (2d Cir. 2010).¹¹

Defendants also argue that because Abadir owned the Cablevision account at the time the auto-forwarding was activated, Cablevision “authorized” him to access Zaratzian’s email, and therefore Zaratzian’s consent was not required. This argument is baseless. First, both of the cases defendants cite for this proposition were decided on the basis of interpretations of specific statutory language that is unique to the SCA—specifically, the exception for “conduct authorized . . . by the person or entity providing a wire or electronic communications service.” 18 U.S.C. § 2701(c). See Connolly v. Wood-Smith, 2012 WL 7809099, at *12 (S.D.N.Y. May 14, 2012), report and recommendation adopted as modified by, 2013 WL 1285168 (S.D.N.Y. Mar. 28, 2013); Cornerstone Consultants, Inc. v. Production Input Solutions, L.L.C., 789 F. Supp. 2d 1029, 1048 (N.D. Iowa 2011). Because the consent exception in the Wiretap Act does not contain this language, these cases have no weight.

Moreover, both cases involved professional email accounts and are thus factually inapposite. Zaratzian had a reasonable expectation of privacy in her personal email, regardless of whether her husband’s name was technically the name on the Cablevision account. To hold otherwise would lead to a perverse outcome in conflict with basic notions of privacy. Cf. Watkins v. L.M. Berry & Co., 704 F.2d at 581 (“Consent under [T]itle III is not to be cavalierly

¹¹ Whether Zaratzian consented to Abadir’s setting of the auto-forwarding function, itself, is also plainly in dispute.

implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place.”).

Accordingly, the Court concludes the scope of Zaratzian’s consent is a genuine issue of material fact.¹²

Abadir’s motion for summary judgment on Zaratzian’s Wiretap Act claims and Zaratzian’s motion for partial summary judgment on the issue of consent are therefore both denied.

C. Carlin

Zaratzian asserts claims against Carlin for disclosing and using the contents of the intercepted June 3, 2009, email under Sections 2511(1)(c) and 2511(1)(d) of the Wiretap Act. Specifically, Zaratzian alleges Carlin disclosed and used Zaratzian’s 2008 tax returns—which Abadir emailed to Carlin on May 18, 2010—by revealing information regarding Zaratzian’s income derived from the returns at a Family Court proceeding in October 2010.

Carlin moves for summary judgment on these claims on the additional basis of Zaratzian’s failure to show Carlin knew or should have known the tax returns Abadir emailed

¹² The Second Circuit’s decision in Anonymous v. Anonymous, 558 F.2d 677 (2d Cir. 1977), does not require dismissal of Zaratzian’s Wiretap Act claims, as defendants urge. In that case, the Second Circuit distinguished the fact pattern before it—a husband taping telephone conversations on his home phone between his daughter, who lived with him, and his wife—from fact patterns in cases from other circuits involving invasions of privacy of “innumerable persons, known and unknown[, which] removed those . . . cases from the province of mere domestic conflicts.” Id. at 679. Here, as in the cases the Second Circuit distinguished, the automatic email forwarding employed by Abadir not only invaded Zaratzian’s privacy—it invaded the privacy of all those who emailed Zaratzian while the forwarding function was activated. Moreover, the Second Circuit explicitly limited Anonymous to the facts it presented. See id. (“[N]or do we suggest that a plaintiff could never recover damages from his or her spouse under the federal wiretap statute. We merely hold that the facts of this case do not rise to the level of a violation of that statute.”). Accordingly, Anonymous does not bar Zaratzian’s claims.

him in 2010 were the product of Abadir's interception of Zaratzian's emails in violation of the Wiretap Act.

Under Sections 2511(1)(c) and 2511(1)(d), it is illegal intentionally to use or disclose the contents of intercepted communications, "knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [Section 2511]." 18 U.S.C. §§ 2511(1)(c), 2511(1)(d). Accordingly, "[t]o be liable under § 2511(1)(c) or § 2511(1)(d), a defendant must know or have reason to know 'sufficient facts concerning the circumstances of the interception such that the defendant[] could, with presumed knowledge of the law, determine that the interception was prohibited in light of [the Wiretap Act].'" McCann v. Iroquois Mem'l Hosp., 622 F.3d 745, 753 (7th Cir. 2010) (quoting Nix v. O'Malley, 160 F.3d 343, 349-50 (6th Cir. 1998)); accord Williams v. Poulos, 11 F.3d 271, 284 (1st Cir. 1993); Thompson v. Dulaney, 970 F.2d 744, 749 (10th Cir. 1992); see also Fernicola v. Specific Real Prop. in Possession, Custody, Control of Healthcare Underwriters Mut. Ins. Co., 2001 WL 1658257, at *7 (S.D.N.Y. Dec. 26, 2001) (Wiretap Act "only prohibits a person from using or disclosing communications where that person knows or has reason to know that the information was obtained in violation of the statute").

Zaratzian contends she has met this standard. In support, she submits evidence of three incidents unrelated to the 2008 tax returns she alleges Carlin used and/or disclosed in violation of the Wiretap Act. Specifically, Zaratzian argues: (i) Carlin communicated with Lendingtree Settlement Services about a refinancing relating to her purchase of Abadir's interest in their former shared residence, and Abadir intercepted several of Zaratzian's emails about that refinancing; (ii) a document Abadir sent Carlin referred to "last week's testament" (meaning Zaratzian's will) and Abadir would have no legitimate reason to know about or have access to

Zaratzian's will; and (iii) one of Zaratzian's attorneys stated Carlin told her that another of Zaratzian's attorneys was "abusing amphetamines" (Doc. #121 ¶ 10), which was apparently the subject of an email received by Zaratzian three years earlier.

Zaratzian urges these three incidents "viewed collectively," together with the email Abadir sent Carlin attaching the tax returns, and Carlin's general involvement in—and resultant familiarity with—the underlying divorce proceedings, lead to an "inference . . . that Carlin had reason to know that the source of Abadir's information was an interception." (Doc. #130 at 3, 5).

The Court disagrees.

When the Court granted Zaratzian's motion for an indicative ruling on her claims against Carlin, the Court concluded the newly-discovered May 18, 2010, email from Abadir to Carlin attaching the tax returns as well as other documents—including a cover letter from Zaratzian's accountant and a "privacy policy" document prepared by the accountant—made Zaratzian's allegations against Carlin plausible. The Court stated, however, it was not making any finding one way or the other as to whether Zaratzian would prevail on her claims against Carlin, and deferred a decision on the merits until discovery had been completed and a summary judgment motion had been filed.

To survive a motion for summary judgment, Zaratzian must present evidence on which a jury could reasonably find for her. Dawson v. Cnty. of Westchester, 373 F.3d 265, 272 (2d Cir. 2004). Summary judgment may be granted for Carlin if the evidence is "merely colorable" or not significantly probative. Anderson v. Liberty Lobby, Inc., 477 U.S. at 249-50.

The evidence Zaratzian submits, taken together, might demonstrate Carlin knew or had reason to know Abadir was obtaining information from Zaratzian by improperly accessing her

computer or email account. Importantly, however, it does not demonstrate Carlin knew enough about the circumstances of the auto-forwarding to allow him to determine Abadir was acquiring Zaratzian's email through that particular method—and without Zaratzian's actual or implied consent—thus providing Carlin enough information to conclude Abadir acquired the tax returns through an interception that violates the Wiretap Act. (Carlin could have concluded, for example, that Abadir had improperly gained access to Zaratzian's computer files, or to her email password, neither of which would violate the Wiretap Act.)

At best, Zaratzian has submitted “merely colorable” evidence in support of her Wiretap Act claims against Carlin, which is not sufficient to defeat summary judgment. Because Zaratzian has failed to make a sufficient showing as to Carlin's knowledge of the circumstances of the interception, summary judgment is appropriate on Zaratzian's claims against Carlin. See Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986).

Carlin's motion for summary judgment on Zaratzian's Wiretap Act claims is therefore granted.

IV. The Stored Communications Act

Under the SCA, “whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished.” 18 U.S.C. § 2701(a).

Defendants argue Zaratzian's SCA claims should be dismissed because, among other reasons, Abadir never “accessed” Zaratzian's email account without authorization—he only logged into his own email account.

Zaratzian does not respond to defendants' summary judgment arguments on the merits of her SCA claims in her opposition brief. The Court therefore deems these claims abandoned. See Hyek v. Field Support Servs., Inc., 702 F. Supp. 2d 84, 102 (E.D.N.Y. 2010) ("Federal courts may deem a claim abandoned when a party moves for summary judgment on one ground and the party opposing summary judgment fails to address the argument in any way." (internal quotation marks omitted)), aff'd, 461 F. App'x 59 (2d Cir. 2012); see also, e.g., McGuire v. Vill. of Tarrytown, 2011 WL 2623466, at *7 (S.D.N.Y. June 22, 2011); Oparaji v. Atl. Container Line, 2008 WL 4054412, at *12 (S.D.N.Y. Aug. 28, 2008), aff'd, 363 F. App'x 778 (2d Cir. 2010).

Zaratzian's SCA claims are therefore dismissed as against both Abadir and Carlin.¹³

V. Constructive Fraud by Fiduciary

Abadir also moves for summary judgment on Zaratzian's claim for "constructive fraud by fiduciary," which Zaratzian asserts against Abadir only. The gravamen of this claim is that Abadir breached a fiduciary duty to Zaratzian by failing to inform her that he was secretly receiving copies of her email messages—including attorney–client communications—before and during the negotiation of their marital separation agreement ("MSA"). Zaratzian alleges this omission damaged her "in that the financial terms of the MSA unreasonably favored Abadir and exceeded that which similarly situated parties in an arms-length transaction would have agreed upon." (SAC ¶ 58).

¹³ Defendants also move for summary judgment on Count Six of the SAC, which is a claim for injunctive relief under Section 2707(b) of the SCA and Section 2520(b) of the Wiretap Act. Because the Court grants defendants' motion for summary judgment on Zaratzian's SCA claims, defendants' motion for summary judgment on Count Six is granted as to both defendants with respect to the SCA. Because the Court denies Abadir's motion for summary judgment—but grants Carlin's motion for summary judgment—on Zaratzian's Wiretap Act claims, defendants' motion for summary judgment on Count Six is, accordingly, denied as to Abadir and granted as to Carlin with respect to the Wiretap Act.

“The elements of common law fraud under New York law are: (1) a material representation or omission of fact; (2) made with knowledge of its falsity; (3) with scienter or an intent to defraud; (4) upon which the plaintiff reasonably relied; and (5) such reliance caused damage to the plaintiff.” DeAngelis v. Corzine, 2014 WL 1695186, at *4 (S.D.N.Y. Apr. 16, 2014) (internal quotation marks omitted). “Constructive fraud requires establishing the same elements as actual fraud except that the element of scienter is replaced by a fiduciary or confidential relationship between the parties.” Id. at *6 (internal quotation marks omitted).

Abadir argues Zaratzian has not met her burden to demonstrate that the omission in question—Abadir’s failure to disclose the auto-forwarding of Zaratzian’s email to his account—caused her damage by adversely affecting the terms of the divorce. The Court agrees.

“To establish causation, plaintiff must show both that defendant’s misrepresentation induced plaintiff to engage in the transaction in question (transaction causation) and that the misrepresentations directly caused the loss about which plaintiff complains (loss causation).” Laub v. Faessel, 745 N.Y.S.2d 534, 536 (1st Dep’t 2002). Abadir contends Zaratzian conceded in her deposition that her theory of damages is entirely speculative and was, moreover, unable to identify any intercepted emails that resulted in her receiving an unfair settlement—or even that discussed “the main terms of the divorce.” (Doc. #135 at 16).

When Abadir was asked at his deposition if emails forwarded from Zaratzian’s account to his account included electronic communications with third parties, including her attorneys, he conceded they did. (See Doc. #126-39 at 18). Nevertheless, even assuming arguendo Zaratzian demonstrated Abadir’s failure to inform her about the auto-forwarding somehow induced her to enter into the MSA (transaction causation), Zaratzian still has not demonstrated loss causation. This is because Zaratzian has submitted no evidence showing how “the financial terms of the

MSA unreasonably favored Abadir” (SAC ¶ 58)—let alone what damages Zaratzian suffered as a result or how Abadir’s failure to disclose his interception of Zaratzian’s emails directly caused any such damages.

Because Zaratzian has therefore failed to make a sufficient showing on loss causation, summary judgment is appropriate on this claim. See Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986).

Abadir’s motion for summary judgment on Zaratzian’s constructive breach of fiduciary duty claim is granted, and Zaratzian’s motion for summary judgment as to the existence of a fiduciary relationship between Abadir and Zaratzian is denied as moot.

CONCLUSION

Defendant Adel Ramsey Abadir's motion for summary judgment is GRANTED in part and DENIED in part.

Defendant Larry M. Carlin's motion for summary judgment is GRANTED.

Plaintiff's motion for partial summary judgment is GRANTED on the narrow issue of whether an interception occurred and is otherwise DENIED.

Plaintiff's claims under the Wiretap Act and for trespass to chattels and violation of New York Penal Law § 250.05 will proceed as against Abadir.

The Clerk is instructed to terminate the pending motions. (Docs. ##110, 114, and 118).

The Clerk is further instructed to terminate defendant Larry M. Carlin.

By October 2, 2014, the parties are directed to submit a joint pretrial order in accordance with the Court's Individual Practices.

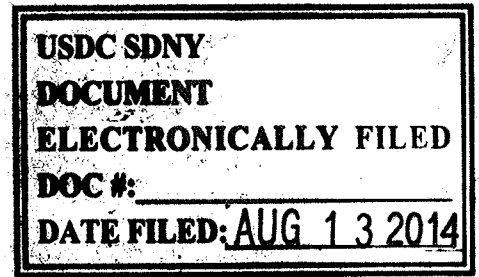
Counsel are directed to attend a status conference on October 16, 2014, at 9:30 a.m., at which time the Court will schedule a trial date.

Dated: September 2, 2014
White Plains, NY

SO ORDERED:

A handwritten signature in black ink, appearing to read 'Vincent Briccetti', written over a horizontal line.

Vincent L. Briccetti
United States District Judge



UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X
AGENCE FRANCE PRESSE,

Plaintiff,

-v-

DANIEL MOREL,

Defendant,

-v-

GETTY IMAGES (US), INC., et al.,

Counterclaim Defendants.
-----X

10-cv-2730 (AJN)

MEMORANDUM &
ORDER

ALISON J. NATHAN, District Judge:

On November 22, 2013, following trial, a jury found that Agence France Presse (“AFP”) and Getty Images (US), Inc. (“Getty,” and together with AFP, “Defendants”¹) had willfully infringed Daniel Morel’s copyright in eight photographs taken in the aftermath of the January 2010 Haiti earthquake. The jury awarded Morel \$303,889.77 in actual damages and infringers’ profits and \$1.2 million in statutory damages. The jury also found that Defendants had committed sixteen violations of the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. §§ 1201–1205, and awarded Morel an additional \$20,000 for those violations. Before the Court

¹ AFP originally brought this action seeking a declaratory judgment that it had not infringed Morel’s photographs. Morel then filed counterclaims against AFP and impleaded Getty as a third-party defendant. (Other third-party defendants that Morel initially named are no longer part of this lawsuit.) Because Morel is alleging violations by AFP and Getty, the Court refers to AFP and Getty as “Defendants” for simplicity’s sake. AFP and Getty were also called “Defendants” at trial to avoid confusing the jury. *See* Dkt. No. 270 at 1 n.2.

is Defendants’ motion under Federal Rules of Civil Procedure 50 and 59(a) for judgment as a matter of law, a new trial, and/or remittitur. Dkt. No. 313. For the following reasons, Defendants’ motion is granted in part and denied in part.

I. Background

The Court assumes familiarity with the facts of this case from its prior opinions on summary judgment and Judge Pauley’s decision at the motion to dismiss stage, when the case was still assigned to him. *Agence Fr. Presse v. Morel*, 769 F. Supp. 2d 295 (S.D.N.Y. 2011) (“*Morel I*”); *Agence Fr. Presse v. Morel*, 934 F. Supp. 2d 547 (“*Morel II*”), *reconsideration granted in part*, 934 F. Supp. 2d 584 (S.D.N.Y. 2013) (“*Morel III*”); Dkt. Nos. 49, 192, 217. Briefly, AFP commenced this action in March 2010 by filing a declaratory judgment complaint naming Morel as the defendant. Morel, a professional photographer who lives in Haiti, had taken a number of photographs on January 12, 2010, in the aftermath of the devastating Haiti earthquake, and uploaded them to Twitter via a TwitPic account. A Twitter user named Lisandro Suero copied the photographs into his own Twitter feed without Morel’s consent, and though the parties dispute precisely what happened next, eight of the photographs—initially credited to Suero—ended up being distributed by AFP and its “image partner” Getty to thousands of news outlets and other customers around the world.

After AFP sought a declaration that it had not infringed Morel’s copyright in the eight photographs,² Morel filed counterclaims against AFP for copyright infringement and violations of the DMCA and the Lanham Act, and also brought third-party claims against Getty and a number of Defendants’ “downstream” customers (no longer parties) who had downloaded the images. On January 14, 2011, Judge Pauley upheld the bulk of Morel’s claims against a motion

² AFP also alleged commercial defamation, but that claim has been voluntarily dismissed. Dkt. No. 34.

to dismiss, but granted the motion with respect to his Lanham Act claims. *Morel I*, 769 F. Supp. 2d at 302–04, 305–06, 308.

On April 27, 2012, following discovery, the remaining parties—at that point, only AFP, Getty, and the Washington Post (“the Post”) were still litigating Morel’s claims—filed cross-motions for summary judgment. This Court rejected as a matter of law Defendants’ primary defense against Morel’s copyright claims, namely, that Defendants were licensed to use Morel’s photographs by virtue of Twitter’s terms of service. That holding meant that AFP and the Post, neither of which had asserted any other defenses, were liable for copyright infringement. The Court also held that genuine issues of material fact precluded judgment on (1) Getty’s remaining defenses against copyright infringement; (2) whether Defendants’ copyright infringement was “willful” so as to trigger enhanced statutory damages under the Copyright Act, *see* 17 U.S.C. § 504(c)(2); (3) Defendants’ secondary liability for the infringements committed by their downstream customers; and (4) Defendants’ liability under the DMCA. *Morel II*, 934 F. Supp. 2d at 564, 568–69, 571–72, 572–75, 578. On reconsideration, the Court clarified that Defendants’ liability for copyright infringement was joint and several, and that Morel could therefore prove at most eight infringements and receive at most eight statutory damages awards—i.e., one per photograph. *Morel III*, 934 F. Supp. 2d at 588–94.

Before trial, Getty dropped its two remaining copyright infringement defenses, thereby conceding liability. The Court also determined that Morel’s secondary liability claims were duplicative, since liability for direct infringement had already been established against both Defendants. Tr. at 870:13–16. Accordingly, the only issues on which the jury was instructed were whether Defendants’ infringements were willful, whether Defendants were liable under the DMCA, and damages under both the Copyright Act and the DMCA.

Trial commenced on November 13, 2013. There were nine witnesses: Morel; Vincent Amalvy, AFP's Director of Photography for North and South America; Eva Hambach, AFP's Deputy to the Director of Photography for North America and South America; Andreas Gebhard, Getty's Editorial Distribution Director; Francisco ("Pancho") Bernasconi, Getty's Vice President for U.S. News and Sports; Katherine Calhoun, Getty's Senior Sales Director for North American Media; Heather Cameron, a Senior Paralegal in Getty's Legal Department; Gilles Tarot, AFP's Director of Sales and Marketing for North America; and Benjamin Fathers, AFP's photo desk chief for Europe and Africa. *See* JPTR Exs. C, D (describing witnesses' roles).

The jury heard testimony from November 14 to November 20, 2013, and delivered its verdict on November 22. It found that both AFP and Getty had willfully infringed Morel's copyright in the eight photographs; awarded Morel \$275,000 in actual damages, \$28,889.77 total in infringing profits, and \$1.2 million in statutory damages; found that AFP and Getty had jointly committed sixteen DMCA violations; and awarded Morel an additional \$20,000 for those violations. Court Exs. 9, 12. On December 10, 2013, after Morel elected to receive statutory damages under the Copyright Act, the Court entered judgment in the amount of \$1,220,000. Dkt. No. 306. The parties submitted a stipulation staying execution of that judgment pending the final disposition of any post-trial motions. Dkt. No. 311.

II. Discussion

Defendants move for judgment as a matter of law on the jury's finding that both AFP and Getty willfully infringed Morel's copyright in the eight photographs, as well as on Morel's DMCA claims. Def. Br. at 4, 12. Defendants also move in the alternative for a new trial on the jury's willfulness finding. *Id.* at 12. Finally, Defendants move for a new trial or remittitur on the jury's damages award for copyright infringement. *Id.* at 20.

A. Legal Standards

Judgment as a matter of law pursuant to Rule 50 is appropriate on a given issue if “a reasonable jury would not have a legally sufficient evidentiary basis to find for” the non-moving party on that issue. Fed. R. Civ. P. 50(a)(1). A court should grant a Rule 50 motion only if “there exists such a complete absence of evidence supporting the verdict that the jury’s findings could only have been the result of sheer surmise and conjecture, or the evidence in favor of the movant is so overwhelming that reasonable and fair minded [persons] could not arrive at a verdict against [it].” *Tepperwien v. Entergy Nuclear Operations, Inc.*, 663 F.3d 556, 567 (2d Cir. 2011) (alterations in original) (quoting *Brady v. Wal-Mart Stores, Inc.*, 531 F.3d 127, 133 (2d Cir. 2008)) (internal quotation mark omitted).

A district court may order a new trial pursuant to Rule 59(a) on the basis that the jury’s verdict was against the weight of the evidence “if and only if” it determines that the verdict is “seriously erroneous” or “a miscarriage of justice.” *Raedle v. Credit Agricole Indosuez*, 670 F.3d 411, 417 (2d Cir. 2012) (quoting *Farrior v. Waterford Bd. of Educ.*, 277 F.3d 633, 634 (2d Cir. 2002)). A court’s discretion to order a new trial includes “overturning verdicts for excessiveness and ordering a new trial without qualification, or conditioned on the verdict winner’s refusal to agree to a reduction (remittitur).” *Kirsch v. Fleet St., Ltd.*, 148 F.3d 149, 165 (2d Cir. 1998) (quoting *Gasperini v. Ctr. for Humanities, Inc.*, 518 U.S. 415, 433 (1996)) (internal quotation mark omitted). “Remittitur is the process by which a court compels a plaintiff to choose between reduction of an excessive verdict and a new trial.” *Lin v. McDonnell Douglas Corp.*, 742 F.2d 45, 49 (2d Cir. 1984)

Generally, remittitur is appropriate under two circumstances: (1) when the court discerns “an error that caused the jury to include in the verdict a quantifiable amount that should be

stricken” or (2) when the award is “intrinsically excessive” in the sense that no reasonable jury could have awarded the amount, whether or not the excessiveness can be attributed to “a particular, quantifiable error.” *Kirsch*, 148 F.3d at 165 (quoting *Trademark Research Corp. v. Maxwell Online, Inc.*, 995 F.2d 326, 337 (2d Cir. 1993)). Where there is no discernible error, the jury’s verdict should be set aside as intrinsically excessive only if “the award is so high as to shock the judicial conscience and constitute a denial of justice.” *Id.* (quoting *O’Neill v. Krzeminski*, 839 F.2d 9, 13 (2d Cir. 1988)) (internal quotation marks omitted).

B. Willful Copyright Infringement

The Copyright Act authorizes a jury to award enhanced statutory damages if it finds that the defendant’s infringement was willful. 17 U.S.C. § 504(c)(2). Infringement is willful if (1) “the defendant was actually aware of the infringing activity” or (2) “the defendant’s actions were the result of ‘reckless disregard’ for, or ‘willful blindness’ to, the copyright holder’s rights.” *Island Software & Computer Serv., Inc. v. Microsoft Corp.*, 413 F.3d 257, 263 (2d Cir. 2005); *see also N.A.S. Imp., Corp. v. Chenson Enterprises, Inc.*, 968 F.2d 250, 252 (2d Cir. 1992) (noting that the defendant’s “knowledge may be ‘actual or constructive.’ In other words, it need not be proven directly but may be inferred from the defendant’s conduct” (citation omitted) (quoting *Fitzgerald Publ’g Co. v. Baylor Publ’g Co.*, 807 F.2d 1110, 1115 (2d Cir. 1986))). In evaluating willfulness, courts look to several factors, including “whether the infringer was on notice that the copyrighted work was protected; whether the infringer had received warnings of the infringements; [and] whether the infringer had experience with previous copyright ownership, prior lawsuits regarding similar practices, or work in an industry where copyright is prevalent.” *Morel II*, 934 F. Supp. 2d at 570 (alteration in original) (quoting *Marshall v. Marshall*, No. 08-cv-1420 (LB), 2012 WL 1079550, at *25 (E.D.N.Y. Mar. 30

2012)) (internal quotation marks omitted). A plaintiff bears the burden of proving willfulness. 17 U.S.C. § 504(c)(2); *Bryant v. Media Right Prods., Inc.*, 603 F.3d 135, 143 (2d Cir. 2010).

Defendants argue that the evidence presented at trial was insufficient for the jury to find that either AFP or Getty committed willful copyright infringement, and that the Court should hold as a matter of law that their infringement was not willful or, alternatively, grant a new trial on that issue. Def. Br. at 4–12. For the reasons that follow, however, the Court will not disturb the jury’s finding that both Defendants’ infringement was willful.

1. AFP’s Willfulness

The evidence was plainly sufficient for the jury to conclude that AFP’s infringement was willful under either an actual knowledge or reckless disregard theory. Amalvy testified that when he sent the pictures from Suero’s Twitter feed to AFP’s photo desk, he believed that Suero was the photographer and that Suero was authorizing Twitter users to distribute the photographs free of charge to bring public attention to the earthquake. Tr. at 308:17–309:9. But the jury was not required to believe Amalvy’s testimony about his mindset, and there was sufficient other evidence indicating that Amalvy took the pictures with reckless disregard for whether he was authorized to do so. Specifically, Amalvy testified that if he had seen Suero’s tweets indicating that Suero was in the Dominican Republic, he would have questioned whether Suero had the right to authorize distribution of the photographs. Tr. at 272:1–6, 18. Although Amalvy said that he did not see these tweets, the jury could conclude from the fact that he sent multiple Twitter messages to Suero on the same night that he did, in fact, see them. Tr. at 281:21–23 (Amalvy). Moreover, even assuming that Amalvy believed the pictures were Suero’s, an email reveals that he felt it was important for AFP to have photographs of the earthquake. Ex. 130A (“I waited a long time before acting, but in my opinion, AFP couldn’t be completely invisible

about a disaster of this magnitude. . . . and *if we had to go there*. . . use the best possible”) (ellipses in original; emphasis added). Amalvy testified to largely the same effect. Tr. at 301:3–302:10. The jury could have concluded from this evidence that Amalvy harbored actual doubts about AFP’s right to use the photographs but went ahead anyway to “salvage the situation” for AFP. Tr. at 302:10.

Perhaps more to the point, AFP concededly became aware, on January 13, that the pictures it had taken from Suero’s Twitter feed had actually been taken by Morel. Tr. at 325:18–326:5 (Amalvy). It also knew, at that point in time, that it did not have permission to use the photographs, given that Morel had never granted such permission. Nonetheless, AFP did not cease distributing the photographs; to the contrary, it issued a caption correction identifying Morel as the photographer and continued to make them available on its feed. Ex. 28; Tr. at 327:8–13 (Amalvy). The fact that AFP apparently took this course of action on the belief that it could work out a deal with Morel at a later date, *see* Def. Br. at 7, does not suggest that it did not know its conduct was infringing. *See Fitzgerald Publ’g Co.*, 807 F.2d at 1115 (“[A] court need not find that an infringer acted maliciously to find willful infringement.”). Indeed, the fact that AFP apparently sought a retroactive license from Morel is arguably *evidence* that it knew, or at least was indifferent to whether, its conduct was infringing; hence the need to seek a release from liability after the fact.

Finally, it also bears noting that AFP works in an industry where copyright was prevalent and has had extensive experience with copyright ownership. Evidence was presented that AFP has guidelines for handling copyright ownership and that the AFP employees implicated in infringing Morel’s copyright were aware of those guidelines. Ex. 144B; Tr. at 275:5–21 (Amalvy). In sum, there was sufficient evidence for the jury to conclude that AFP’s

infringement was willful. The Court therefore denies Defendants' Rule 50 motion with respect to AFP's willfulness. In light of the evidence described above, the Court also concludes that the jury's verdict was not seriously erroneous or a miscarriage of justice, and therefore denies Defendant's motion for a new trial on AFP's willfulness.

2. Getty's Willfulness

The evidence showed that Suero-credited versions of Morel's photographs remained available to Getty customers as late as February 2, 2010, roughly two and a half weeks after AFP sent a "kill notice" asking Getty to remove all "Daniel Morel pictures from Haiti" from Getty's systems. Ex. 54. And between receiving the kill notice on January 14 and pulling the remaining images from its website on February 2, Getty licensed these Suero-credited images to its customers numerous times. Getty's willfulness therefore turns on whether it knew that the Suero-credited images were still available for sale on its site even after receiving the kill notice and removing Morel-credited images. Although the evidence of Getty's willfulness is somewhat thin in comparison to the evidence regarding AFP's willfulness, the Court concludes that it was sufficient to support the jury's verdict.

On January 13, AFP sent a "caption correction" to Getty in order to credit Morel's photographs to Morel instead of Suero. Ex. 28, 29. There was evidence that Gebhard, who was responsible for removing the infringing photographs from Getty's website after it received the kill notice from AFP on January 14, was aware that AFP had sent the caption correction on the same photographs a day earlier. Specifically, in a response to a January 14 email from Hambach notifying various Getty employees of the kill notice, Gebhard recognized that AFP had "correct[ed] the photogs [sic] name" the day before. Ex. 55; Tr. at 537:5–539:22 (Gebhard). Gebhard claimed that he had not actually seen the substance of AFP's caption correction;

instead, he testified that when he was searching for Morel-credited photographs in response to the kill notice, he saw that some were credited to “David Morel” and inferred (apparently without further investigation) that the caption correction was meant to correct “David” to “Daniel.” Tr. at 539:23–540:7. But the jury did not have to believe this explanation; it could have concluded, based on Gebhard’s email, that he actually had seen the substance of the caption correction and therefore knew that Suero-credited versions of Morel’s photographs had been made available to Getty’s customers. In that case, Gebhard’s failure to search for or remove those Suero-credited images from Getty’s website would be sufficient evidence of willfulness. *See Morel II*, 934 F. Supp. 2d at 571.

Defendants point out that AFP’s kill notice neither specified the image numbers of the infringing photographs nor mentioned Suero, and that AFP had sent multiple copies of Morel’s photographs to Getty, making it difficult for Gebhard to know whether he had actually removed all of the images (whether credited to Suero or Morel) from Getty’s website. Def. Br. at 9; Def. Reply at 5–6 & n.5. But the kill notice’s failure to mention Suero is irrelevant if Gebhard knew that AFP had sent Suero-credited pictures, and the vagueness of the kill notice cuts both ways—it arguably suggests that Gebhard should have been more meticulous in finding and removing Morel’s photographs. That is particularly true in light of the fact that Gebhard had seen the photographs on Morel’s Twitter feed the night of the earthquake. *See Ex. 2*. The jury therefore could have concluded that Gebhard would have been able to identify the pictures just by looking. Accordingly, the alleged shortcomings of the kill notice do not preclude willfulness as a matter of law; they at most raised an additional factual issue for the jury.

Furthermore, as with AFP, there was evidence that Getty in general, and Gebhard in particular, were familiar with copyright and worked in an industry where copyright was

prevalent. *E.g.*, Tr. at 543:7–547:1 (Gebhard). That evidence further buttresses the jury’s willfulness finding.

Defendants cite two cases for the proposition that Getty’s actions amount to mere negligence, not willfulness, but these cases are distinguishable. In *Video Views, Inc. v. Studio 21, Ltd.*, 925 F.2d 1010 (7th Cir. 1991), *overruled on other grounds by Fogerty v. Fantasy, Inc.*, 510 U.S. 517 (1994), the court agreed with the district court that the defendant’s infringement was not willful as a matter of law because although the defendant had received notice that the plaintiff owned the copyright in certain videos produced by twelve companies, the two videos it allegedly infringed were not produced by any of those companies. *Id.* at 1020–21. The specific reference to *other* copyrighted works could not have put the defendant on notice with respect to the two infringed works. In this case, by contrast, AFP’s kill notice did not convey any similar negative implication. It may have been vague, but it identified the correct copyright owner, and given the evidence suggesting that Gebhard actually knew that Getty was distributing Suero-credited photographs, the notice’s failure to mention Suero is irrelevant. *King Records, Inc. v. Bennett*, 438 F. Supp. 2d 812 (M.D. Tenn. 2006), was decided after a bench trial and therefore applies the wrong standard. This Court’s task is not to arrive at the best view of the evidence, but rather to determine whether the jury’s findings were supportable.

Because the Court concludes that there was sufficient evidence to find Getty liable for willful copyright infringement, Defendants’ motion for judgment as a matter of law on that issue is denied. The Court also denies Defendants’ motion for a new trial on Getty’s willfulness. In light of the evidence discussed above, the jury’s verdict rested significantly on its assessment of the Getty witnesses’ credibility. The Second Circuit has cautioned that while district courts may weigh evidence in considering Rule 59 motions, they should exercise this ability “with caution

and great restraint, as a judge ‘should rarely disturb a jury’s evaluation of a witness’s credibility,’ and may not ‘freely substitute his or her assessment of the credibility of witnesses for that of the jury simply because the judge disagrees with the jury.’” *Raedle*, 670 F.3d at 418 (citations omitted) (quoting *DLC Mgmt. Corp. v. Town of Hyde Park*, 163 F.3d 124, 134 (2d Cir. 1998); and *United States v. Landau*, 155 F.3d 93, 104 (2d Cir. 1998)). The Court declines to hold that the jury’s assessment of the evidence in this case, turning as it did on the witnesses’ credibility, was seriously erroneous or a miscarriage of justice.

C. DMCA Liability

Defendants argue that the evidence was insufficient to find them liable for violating the DMCA. The jury was instructed on two theories of DMCA liability, which the parties refer to as “providing or distributing” false copyright management information (“CMI”), and “altering” CMI. These two theories correspond to two subsections of the DMCA.

First, the DMCA makes it unlawful to knowingly, and with the intent to “induce, enable, facilitate, or conceal infringement,” either “provide” or “distribute” (or “import for distribution”) false CMI. 17 U.S.C. § 1202(a). Thus, under this subsection, § 1202(a), the defendant must both know that the CMI is false, and provide or distribute the false CMI with the intent to induce, enable, facilitate, or conceal infringement. *See Ward v. Nat’l Geographic Soc’y*, 208 F. Supp. 2d 429, 449 (S.D.N.Y. 2002).

Second, the DMCA also prohibits doing any of the following “without the authority of the copyright owner or the law” and with knowledge or reasonable grounds to know that it will “induce, enable, facilitate, or conceal” infringement:

- (1) intentionally remove or alter any copyright management information,

(2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or

(3) distribute . . . works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law.

17 U.S.C. § 1202(b). As relevant here, the definition of CMI includes “[t]he name of, and other identifying information about, the author of a work,” and “[t]he name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.” *Id.* § 1202(c)(2), (3).

Defendants challenge the jury’s finding that AFP and Getty jointly committed eight violations of each subsection, for sixteen total DMCA violations. Def. Br. at 12–15. As explained below, the Court agrees with Defendants only in part. Specifically, there was insufficient evidence to find Getty liable for violating § 1202(b). Otherwise, the evidence was sufficient to support the jury’s verdict.

1. AFP’s DMCA Liability

Much of the same evidence on which the jury could have found that AFP’s infringement was willful also permitted the jury to find AFP liable under both relevant subsections of the DMCA. First, there was evidence that AFP “provided or distributed” false CMI with the intent to induce, enable, or facilitate, or conceal infringement. 17 U.S.C. § 1202(a). As noted, the jury could have concluded based on Amalvy’s January 12 Twitter activity that he knew the eight images were not Suero’s from the beginning yet falsely credited them to Suero. Additionally, even if AFP’s addition of the identifier “AFP” to Morel’s images did not imply that AFP itself was the copyright owner, there was sufficient evidence that it conveyed false “identifying information about” the “author of a work,” 17 U.S.C. § 1202(c)(1), by implying that Morel was

associated with AFP, which he was not. *See* Ex. 328 (email from Corbis suggesting that the “Getty Images” identifier on Morel’s photographs suggested that Morel was associated with Getty); Tr. at 175:6–17 (Morel); *see also Morel II*, 934 F. Supp. 2d at 577 (finding a genuine factual issue with respect to whether “AFP” and “Getty Images” identifiers added by Defendants “convey[ed] information about copyright ownership” and therefore qualified as CMI).³ And the jury could have concluded that AFP acted with the required intent by providing and distributing the false CMI in order to license Morel’s photographs to its customers. *See Morel II*, 934 F. Supp. 2d at 578 (citing *McClatchey v. Associated Press*, No. 05-cv-145, 2007 WL 776103, at *6 (W.D. Pa. Mar. 9, 2007)).

Second, there was also evidence that AFP “alter[ed]” the CMI on Morel’s photographs without Morel’s authority and distributed copies of Morel’s images knowing that the CMI had been altered without his authority. 17 U.S.C. § 1202(b)(1), (2). The evidence showed that after AFP became aware that Suero was not the author of the eight images, AFP issued a caption correction identifying Morel as the photographer and continued to make the images available to its customers. When it issued that caption correction, AFP concededly had not received permission from Morel to either distribute his photographs or make the correction. From this evidence, the jury could have concluded that in continuing to distribute the photographs with a

³ Defendants previously argued that the identifiers should be covered by language in the DMCA providing that the definition of CMI does not include “any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work.” 17 U.S.C. § 1202(c). The Court reserved on that argument during trial, Tr. at 899:7–17, but Defendants do not appear to have renewed it in their post-trial briefing. *See Kirsch*, 148 F.3d at 164 (“As to any issue on which no proper Rule 50(b) motion was made, JMOL may not properly be granted by the district court . . . unless that action is required in order to prevent manifest injustice.”). In any event, although the Court has been unable to find any definition of § 1202(c)’s term “user,” the definition is irrelevant in light of the Court’s conclusion that the jury could have found that the identifiers *did* convey “identifying information about” the “author of the work.” *See* Tr. at 845:14–15 (observing that Defendants’ “user” argument was “not a statutory argument . . . but an evidentiary argument”)

caption identifying Morel as the photographer, AFP had both altered the “name of . . . the author of” the photographs, 17 U.S.C. § 1202(c)(2), without the authority of the copyright owner, and had distributed Morel’s images while knowing that their CMI had been altered without his authority. And the jury could have concluded that AFP knew or had reasonable grounds to know that its alteration of CMI would “induce, enable, or facilitate infringement” by enabling the continued licensing of Morel’s images—which were now credited to Morel but still not AFP’s to license—to AFP’s customers. Defendants’ contention that AFP “was trying to correct its mistake,” Def. Reply at 11 (emphasis omitted), does not imply that it did not know its activities were infringing or that it was not facilitating infringement.

2. Getty’s DMCA Liability

The evidence supporting the jury’s willfulness finding with respect to Getty’s copyright infringement was also sufficient to support its finding that Getty violated § 1202(a) of the DMCA. Specifically, if Gebhard knew that the Suero-credited photographs were still available on Getty’s feed yet failed to remove them after receiving AFP’s kill notice, the jury could have concluded that he did so with the intent to enable the continued licensing of the Suero-credited images to Getty’s customers. On that view of the facts, Gebhard also would have known, at the point when he failed to remove the images from Getty’s feed, that CMI associated with the Suero-credited images—the Suero credit and “AFP” and “Getty Images” identifiers—was false. Accordingly, there was sufficient evidence for the jury to conclude that Getty’s continued distribution of the Suero-credited images following AFP’s kill notice satisfied all of the elements required by § 1202(a). *See Morel II*, 934 F. Supp. 2d at 578 & n.19 (identifying a triable issue of fact on Getty’s DMCA liability in light of evidence involving Gebhard’s knowledge of the Suero-credited images).

However, there was insufficient evidence to find Getty liable under § 1202(b) of the DMCA. Initially, the Court agrees with Defendants that the addition of the identifiers “AFP” and “Getty Images” cannot constitute *removal* or *alteration* of CMI—both of those words suggest that a defendant must take some action with respect to pre-existing CMI. *See Webster’s Third New International Dictionary* 63 (2002 ed.) (defining “alter” as “to cause to become different in some particular characteristic”); *id.* at 1921 (defining “remove” as “to move by lifting, pushing aside, or taking away or off”). On that interpretation, the evidence showed that there were only two ways in which CMI on Morel’s photographs was altered or removed without his authority: when Suero first took the images from Morel’s TwitPic feed and removed the identifying information that accompanied the images on that feed, *see* Ex. 141A; *Morel I*, 769 F. Supp. 2d at 305–06 (rejecting argument that attributions “Morel” and “by photomorel” on Morel’s TwitPic page were not CMI), and when, as described above, AFP changed the photographer credit on the photographs from Suero to Morel. Although Getty itself did not participate in these actions, it might still be liable if it distributed the images knowing that the CMI had been altered or removed without Morel’s consent. *See* 17 U.S.C. § 1202(b)(3); *Morel II*, 934 F. Supp. 2d at 578 n.19.

But even if the jury believed that Gebhard knew there were images on Getty’s feed that were wrongly credited to Suero even after AFP’s kill notice, there was no evidence that he or anyone else at Getty knew that Suero had removed the TwitPic CMI from Morel’s photographs. And there was no evidence that Getty knew Morel had not given AFP authority to change the photographer credit from Suero to Morel when AFP sent the caption correction; even if that lack of authority could have been inferred from the subsequent kill notice, there was no evidence that Getty continued to distribute *Morel*-credited images (as opposed to Suero-credited images) post–

kill notice. Because there was therefore insufficient evidence supporting the jury's finding that Getty acted with the knowledge required by § 1202(b), the Court concludes as a matter of law that Getty was not liable under that subsection.

D. DMCA Damages

In addition to challenging the sufficiency of the evidence on DMCA liability, Defendants raise two broad arguments with respect to the jury's DMCA damages award. Like the Copyright Act, the DMCA allows a plaintiff to choose between recovering actual damages and statutory damages. 17 U.S.C. § 1203(c)(1), (3). For violations of 17 U.S.C. § 1202 (the section of the DMCA at issue here), the DMCA provides that a plaintiff "may elect to recover an award of statutory damages for each violation . . . in the sum of not less than \$2,500 or more than \$25,000." *Id.* § 1203(c)(3)(B). The jury awarded Morel \$20,000 for sixteen DMCA violations, finding that he suffered actual damages of \$20,000 and awarding him \$20,000 in statutory damages. Court Ex. 9 at 6, 7; Court Ex. 13. Although Morel has noted that this is actually less than the \$40,000 minimum that a jury may award as statutory damages, Dkt. No. 287, he has not filed any post-trial motions addressing this point. The Court will therefore consider it abandoned and turn to Defendants' arguments. *See* Dkt. No. 305 (indicating that any objections to the amount of the jury's award "must be made by appropriate post-trial motion").

First, Defendants repeat their argument, originally advanced in a motion in limine, that recovering multiple awards under the DMCA requires a plaintiff to prove that he has suffered a distinct injury traceable to each violation. Def. Br. at 18–20. Defendants ground this argument in the statutory language, which provides that "[a]ny person *injured by a violation* of section 1201 or 1202 may bring a civil action in an appropriate United States district court *for such violation*." 17 U.S.C. § 1203(a) (emphasis added). The Court has already rejected this precise

argument, holding instead that the DMCA defines “violation” on a work-by-work basis and thus allows a plaintiff to recover one award per work infringed without demonstrating a separate injury as to each. Tr. at 893:1–896:16. This interpretation largely harmonizes the DMCA’s statutory damages scheme with the Copyright Act’s and is consistent with (limited) case law addressing the issue. *See Propet USA, Inc. v. Shugart*, No. 06-cv-186, 2007 WL 4376201, at *5 (W.D. Wash. Dec. 13, 2007); *Stockart.com, LLC v. Engle*, No. 10-cv-588, 2011 WL 10894610, at *14 (D. Colo. Feb. 18, 2011), *adopted*, No. 10-cv-588 (D. Colo. Apr. 7, 2011), ECF No. 63. The “injury” language that Defendants emphasize is better read as defining the class of plaintiffs who may sue for a given DMCA violation. Tr. at 894:24–895:22. Defendants have not cited any new authority or advanced any persuasive new arguments in their post-trial briefing, so the Court will not reconsider its earlier holding.⁴

Second, Defendants argue that Morel may not recover for any DMCA violations because there was insufficient evidence for the jury to conclude that he suffered an injury separate and apart from the injuries attributable to Defendants’ copyright violations. Def. Br. at 16–18. Defendants are correct that the law ordinarily forbids a plaintiff from recovering twice for the same injury. *See Indu Craft, Inc. v. Bank of Baroda*, 47 F.3d 490, 497 (2d Cir. 1997). But they have never argued that DMCA damages will *always* be duplicative of an award for copyright infringement,⁵ and therefore recognize that in an appropriate case, separate DMCA and copyright awards might be permissible. *See* Dkt. No. 252 at 16 n.12; Tr. at 898:20–24. This is true because the Copyright Act and the DMCA protect different interests. Accordingly, the jury was

⁴ Given that this issue has already been decided, the Court disagrees with Defendants’ contention that Morel has “tacitly conceded” their single-award argument by addressing it only in a footnote. Def. Reply at 13 n.12.

⁵ For this reason, cases rejecting offhand the possibility of dual awards under the two statutes are inapposite in the context of this case. *E.g., Adobe Sys. Inc. v. Feather*, 895 F. Supp. 2d 297, 303 n.5 (D. Conn. 2012).

instructed that “if you find that Mr. Morel is entitled to a verdict on both his copyright infringement and his DMCA claims, you may not compensate him twice for any harm he might have suffered.” Court Ex. 3 at 29. The jury must be presumed to have determined that Morel suffered additional harm beyond what he suffered as a result of Defendants’ copyright infringement. *See, e.g., Richardson v. Marsh*, 481 U.S. 200, 211 (1987) (noting the presumption that juries follow their instructions).

Defendants argue that even if the jury was correctly instructed, there was insufficient evidence supporting its finding that Morel suffered \$20,000 in actual damages. However, the Court concludes that it need not address the sufficiency of the evidence on this point because it is irrelevant to whether the jury’s *statutory* damages award (of the same amount) was appropriate. With respect to statutory damages under the DMCA, the jury was instructed, consistent with the parties’ proposed jury instructions, *see* JPTR Ex. I at 69–70, that it was entitled to consider other factors in addition to Morel’s actual damages, namely, the difficulty of proving actual damages, the circumstances of the violation, whether Defendants violated the DMCA intentionally or innocently, and deterrence. Court Ex. 3 at 32. In the context of the Copyright Act, it is clear that statutory damages can be awarded even in the absence of sufficient evidence supporting actual damages, *see Columbia Pictures Television, Inc. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1194 (9th Cir. 2001), and the Court likewise sees no reason why an inadequately supported claim of actual damages should preclude Morel from recovering statutory damages under the DMCA. In light of all the factors the jury was entitled to consider, its statutory award of \$20,000—or half the statutory *minimum*—was permissible.

E. Copyright Damages

The Copyright Act permits a plaintiff to choose between receiving an award of (1) compensatory damages, in the form of actual damages plus the infringer's profits or (2) statutory damages. *See* 17 U.S.C. § 504(a), (c).

The two categories of compensatory damages—actual damages and infringer's profits—are distinct: “any profits of the infringer that are attributable to the infringement” cannot be “taken into account in computing the actual damages.” *Id.* § 504(b).

The award of the infringer's profits examines the facts only from the infringer's point of view. If the infringer has earned a profit, this award makes him disgorge the profit to insure that he not benefit from his wrongdoing. The award of the owner's actual damages looks at the facts from the point of view of the copyright owner; it undertakes to compensate the owner for any harm he suffered by reason of the infringer's illegal act.

Davis v. The Gap, Inc., 246 F.3d 152, 159 (2d Cir. 2001). In assessing actual damages, a factfinder may look to the profits that the plaintiff lost because of the infringement, any diminution in the market value of the plaintiff's copyright, or what the plaintiff would have received as a reasonable licensing fee for the defendant's infringing use. *See id.* at 164–66; *Fitzgerald Publ'g Co.*, 807 F.2d at 1118–19. Actual damages “should be broadly construed to favor victims of infringement,” *Davis*, 246 F.3d at 164, but a jury's actual damages award also cannot be “based upon undue speculation,” *Abeshouse v. Ultragraphics, Inc.*, 754 F.2d 467, 470 (2d Cir. 1985).

As an alternative to an award of actual damages plus infringer's profits, a plaintiff may elect to recover statutory damages at any time before a final judgment is rendered. 17 U.S.C. § 504(c). The Copyright Act prescribes three ranges for statutory damages, depending on whether the infringement was innocent, willful, or neither. The statutory damages range is \$200 to \$30,000 per work for innocent infringement, \$750 to \$150,000 per work for willful

infringement, and \$750 to \$30,000 per work for regular infringement. *See id.* The Second Circuit has prescribed six factors to be considered in setting statutory damages within these ranges: “(1) the infringer’s state of mind; (2) the expenses saved, and profits earned, by the infringer; (3) the revenue lost by the copyright holder; (4) the deterrent effect on the infringer and third parties; (5) the infringer’s cooperation in providing evidence concerning the value of the infringing material; and (6) the conduct and attitude of the parties.” *Bryant*, 603 F.3d at 144.

On Morel’s copyright claims, the jury awarded him \$275,000 in actual damages, plus \$28,889.77 total in infringing profits (\$14,447.76 for AFP and \$14,442.01 for Getty) or, alternatively, \$1.2 million in statutory damages—the maximum possible statutory award for the willful infringement of eight works. Following trial, Morel elected to receive statutory damages. Dkt. No. 287. Defendants make two arguments for a new trial or remittitur. First, they argue that the jury’s actual damages award of \$275,000 was overly speculative and therefore amounts to a discernible error that would justify remittitur. Def. Br. at 20. Second, they argue that the \$1.2 million statutory damages award was intrinsically excessive in light of the evidence. *Id.* at 25. For the following reasons, the Court rejects both arguments.

1. Actual Damages

As a preliminary matter, it is important to note that because Morel has (understandably) elected to receive statutory damages, Defendants are challenging the jury’s actual damages calculation primarily insofar as it undergirds the jury’s \$1.2 million statutory damages award. If the Court were to conclude that the jury’s statutory damages award was excessive, Defendants appear to concede that as much as \$400,000 would be an appropriate award following remittitur—at least in light of the Court’s holding that the evidence was sufficient to find that Defendants’ infringement was willful. *See* Def. Br. at 31–32 (urging the Court to rely on cases

rewarding between \$20,000 and \$50,000 in statutory damages per work for willful infringement). One would, of course, expect Morel to elect statutory damages of \$400,000 over actual damages of \$275,000, so only statutory damages would be relevant even if the Court were to side with Defendants.

But as Defendants point out, actual damages may be relevant even if a plaintiff elects to recover statutory damages. *See Bryant*, 603 F.3d at 144 (listing “the revenue lost by the copyright holder” among the factors to be considered in setting statutory damages). Defendants argue that the jury’s inappropriate actual damages calculation “infected” its \$1.2 million statutory damages award, thereby furnishing one of several grounds on which the Court should remit that award. Def. Br. at 20. That is because “actual damages is one of the *Bryant* factors, and . . . there must be some correlation between actual damages and statutory damages.” Def. Reply at 8. Thus, in Defendants’ view, the jury’s statutory damages award must be set aside because it is based in part on a faulty actual damages calculation. The Court disagrees.

To begin with, Defendants’ premise that an overly speculative actual damages award is a discernible error justifying remittitur is questionable for at least two reasons. First, it is not true that there must be “some correlation” between actual and statutory damages. The Second Circuit recently rejected a defendant’s argument that the district court abused its discretion in denying remittitur because the award had no “rational relationship” to the plaintiff’s damages. *Psihoyos v. John Wiley & Sons, Inc.*, 748 F.3d 120, 126 (2d Cir. 2014) (“*Psihoyos II*”). The Court noted:

Although revenue lost is one factor to consider, we have not held that there must be a direct correlation between statutory damages and actual damages. To suggest otherwise is to ignore the various other factors a court may consider and the purposes of statutory damages in the willful infringement context.

Id. at 127. The court agreed with the district court that other factors, such as the defendant’s profits and a perceived need for deterrence, could have justified the award. *Id.*; accord *Yurman*

Design, Inc. v. PAJ, Inc., 262 F.3d 101, 113 (2d Cir. 2001) (upholding jury’s statutory damages award that defendant argued bore “little relationship” to actual damages because “even if [defendant’s] accounting is correct, statutory damages are not meant to be merely compensatory or restitutionary”); *L.A. Printex Indus., Inc. v. Does 1–10*, 543 F. App’x 110, 111 (2d Cir. 2013); *Sony BMG Music Entm’t v. Tenenbaum*, 660 F.3d 487, 506–07 (1st Cir. 2011). As explained in more detail below, the jury’s statutory damages award in this case could have been based on a number of factors, so the Court cannot discern a “quantifiable amount,” *Kirsch*, 148 F.3d at 165, by which any mistake in the jury’s actual damages calculation might have “infected” its statutory damages award.⁶

Second, even accepting the premise that there must be “some correlation” between actual and statutory damages, Defendants’ argument that the actual damages calculation is overly speculative is a questionable basis for attacking a statutory damages award, for reasons that the Court explained in addressing the parties’ motions in limine. Because “statutory damages are by definition a substitute for unproven and unprovable damages,” *Psihoyos v. John Wiley & Sons, Inc.*, No. 11-cv-1416 (JPO), 2012 WL 5506121, at *3 (S.D.N.Y. Nov. 7, 2012) (“*Psihoyos I*”) (quoting *Capitol Records, Inc. v. Thomas-Rasset*, 692 F.3d 899, 909–10 (8th Cir. 2012)), a less stringent standard may govern the consideration of actual damages evidence insofar as that evidence bears only on statutory damages. If that is true, then Defendants’ argument regarding

⁶ Indeed, the First Circuit has approved a district court’s instructions that the jury should arrive at statutory damages by considering what was “just,” guided by a “set of non-exhaustive factors” similar to the *Bryant* factors. *Tenenbaum*, 660 F.3d at 503–04. That suggests that a jury need not even consider a plaintiff’s actual damages at all in setting statutory damages, *see also* 5 Nimmer on Copyright § 14.04[B][1][a] (suggesting that factors guiding statutory damages awards apply “[i]n the absence of a jury trial”), which would further suggest that an erroneous actual damages award is not a discernible error justifying remittitur. The Court’s jury instructions in this case were consistent with the First Circuit’s analysis in *Tenenbaum*, *see* Court Ex. 3 at 21 (instructing that the jury “may consider any or all” of the *Bryant* factors), and Defendants did not object to them.

speculativeness—which relies on cases involving actual damages qua actual damages, Def. Br. at 21 & n.11—would be inapposite. *Cf. Columbia Pictures Television*, 259 F.3d at 1194 (“A plaintiff may elect statutory damages ‘regardless of the adequacy of the evidence offered as to his actual damages and the amount of the defendant’s profits.’” (quoting 5 Nimmer on Copyright § 14.04[A])). However, just as it was unnecessary to resolve that question earlier, it is also unnecessary now, because there was sufficient evidence for the jury to conclude that Morel suffered \$275,000 in actual damages.

Defendants base their analysis on the assumption that the jury concluded that Morel would have sold 1,000 licenses for his photos at an average of \$275 per license. But that is not necessarily correct. There was evidence that AFP and Getty licensed the images for up to \$1,450 each, *see* Ex. 264C at row 29, and assuming that Morel himself had received the same amount per license, he would have had to make fewer than 200 sales to have generated \$275,000. Additionally, Morel testified that one offer he received from NBC would have paid him \$500 for a single photograph. Tr. at 171:13–20, 176:19–177:1 (Morel).

In any case, there was enough evidence for the jury to conclude that Morel would have made 1,000 sales: that was roughly the number of customers who, the evidence showed, obtained the images from Defendants. Exs. 137, 138, 264C, 265C; Tr. at 727:16–17, 729:4–732:5 (Calhoun); Tr. at 785:18–791:2 (Tarot). The Court cannot say that it was irrational to infer that all of the AFP and Getty customers that downloaded the pictures would have bought them from other sources. *See Stevens Linen Assocs., Inc. v. Mastercraft Corp.*, 656 F.2d 11, 15 (2d Cir. 1981) (endorsing damages theory that would calculate damages by assuming defendants’ customers would have bought from plaintiff but for defendant’s infringement); *RSO Records, Inc. v. Peri*, 596 F. Supp. 849, 860 (S.D.N.Y. 1984) (“It would be reasonable to assume that for

every counterfeit copy of plaintiffs' copyrighted records and tapes sold by defendants plaintiffs lost a corresponding sale."'). The earthquake was a major news event, and there was evidence that pictures from on the ground were difficult to come by in its immediate aftermath. Tr. at 301:3–302:10 (Amalvy). In other words, it would be reasonable to conclude that there would have been demand for Morel's photographs had Defendants not made them widely available to their customers. That is particularly true in light of testimony that NBC reneged on its offer to Morel because it had obtained the image from AFP. Tr. at 171:17–22 (Morel).

Although Defendants point out that the total number of downloads by AFP and Getty customers—roughly 1,000—included “downloads by *both* a la carte customers and subscription customers who purchased their subscriptions long before Morel's photographs even existed,” that argument misses the mark. Def. Br. at 24. Initially, it is worth noting that the 1,000-download figure appears to understate the true number of downloads; while there was evidence presented at trial about Getty's subscription downloads, *see* Ex. 265C; Tr. at 728:20–729:1 (Calhoun), Tarot testified that there was no way of knowing which of AFP's subscription (as opposed to a la carte) customers had downloaded the images. Tr. at 787:13–788:2. And the Court's prior holding that fees paid by Defendants' subscribing customers could not be used to calculate Defendants' infringing profits is irrelevant to Morel's actual damages; it was based on the fact that subscribers paid in advance for the right to download images from Defendants' feeds, so revenue generated by those subscriptions could not logically be attributable to the dissemination of Morel's images. That does not imply that Defendants' subscription customers would not have paid Morel—or his agency, Corbis—for the photographs had the photographs not already been made available to them through their AFP or Getty subscriptions. Indeed, at the November 20, 2013 charging conference, the Court agreed with *Defendants'* suggestion that the

value placed on Morel's photographs by subscription customers would be "appropriately considered in calculating actual damages." Tr. at 892:4–7.

Defendants point out that Morel himself received only one offer to buy a photograph, but of course he might have received more had Defendants themselves not made his photographs widely available. And although there is some merit to Defendants' argument that Morel's spotty internet and phone access would have made it difficult for him to close numerous sales after the earthquake, the evidence showed that Corbis was marketing his photos as well. Assuming that all 1,000 sales were made through Corbis,⁷ Morel would not have received the entirety of the proceeds from those sales under his existing contract; he received only 50% of Corbis's revenue from sales for "editorial use" and 45% of its revenue from sales for "commercial use." Ex. 303 at 000189; Tr. at 211:4–8 (Morel). But as noted, there was other evidence from which the jury could have concluded that the per-license fee was higher than \$275. Assuming that Morel received 50% of the revenues from Corbis's 1,000 sales, those sales would have had to average \$550 to generate \$275,000 in lost profits. That is just \$50 higher than NBC offered Morel, and significantly lower than the \$1,450 that Getty received for one sale. Ex. 264C at row 29. There was therefore evidence from which the jury could conclude that Morel lost \$275,000 in sales even if all those sales were made through Corbis.⁸

⁷ Defendants also argue that Corbis would have earned only \$29,000 from licensing the photos—the same amount made by Defendants themselves. Def. Br. at 22–23; Def. Reply at 7. But that argument incorrectly assumes that the number of licenses Corbis could have sold would have equaled only the number of a la carte sales that Defendants made. As noted, had Defendants' subscription customers bought the photographs from Corbis, they would not have been able to obtain the photos based on already-paid subscription fees.

⁸ Although Defendants do not argue that the jury double counted, it arguably would have been wrong for the jury to include Defendants' a la carte customers in the number of sales Morel or Corbis would have made, because sales to a la carte customers were already accounted for in Defendants' infringing profits; indeed, because the Court precluded the jury from attributing subscription revenues to Defendants' infringement, a la carte fees composed the entirety of those profits. But even if one excludes Defendants' a la carte customers from the total number of sales that Morel or Corbis would have made but for Defendants' infringement, the range of prices at which Defendants

For these reasons, the Court cannot conclude that the jury's actual damages award was impermissibly speculative. As a result, that award also cannot be a basis for remitting the jury's statutory damages award.

2. Intrinsic Excessiveness

Apart from the actual damages calculation that Defendants argue "infected" the jury's statutory damages award, Defendants also argue that the Court should remit the \$1.2 million award as intrinsically excessive. Although, in general, a damages award may be set aside if it is "so high as to shock the judicial conscience and constitute a denial of justice," this is a "narrow standard." *O'Neill*, 839 F.2d at 13 (quoting *Zarcone v. Perry*, 572 F.2d 52, 56 (2d Cir. 1978)) (internal quotation mark omitted). And in the specific context of statutory damages under the Copyright Act, Congress has placed an upper bound on the damages that a jury can award, which mitigates the risk of a truly untethered award. Defendants concededly cite only one case in which a court has overturned a jury's statutory damages award as excessive where the award is within the statutory guidelines.⁹ Def. Reply at 9. It is true that courts setting statutory damages

sold the photographs, and the fact that there were likely more than 1,000 downloads in total, was sufficient evidence from which the jury could have concluded that even the total number of sales would have been at a high enough rate to amount to \$275,000 in total.

⁹ That case, *Capitol Records Inc. v. Thomas-Rasset*, 680 F. Supp. 2d 1045 (D. Minn. 2010), is of limited relevance in any event. The district court conducted three trials. After the first, at which the jury granted \$222,000 in damages, the district court concluded that it had erred in instructing the jury on liability and ordered a new trial. At the second trial, the jury awarded the plaintiff \$1.92 million in statutory damages, and the court remitted the amount to three times the statutory minimum, *see id.* at 1054–57, but the plaintiff rejected the remitted amount and another trial was held. At that third trial, the jury awarded the plaintiff \$1.5 million, and the district court rejected the award as violating due process—rather than on common law remittitur grounds—and again held that three times the statutory minimum was the maximum permissible award. *Capitol Records, Inc. v. Thomas-Rasset*, 799 F. Supp. 2d 999, 1011–14 (D. Minn. 2011) ("*Thomas-Rasset II*"). That decision was vacated by the Eighth Circuit; on appeal, however, the plaintiff sought only the original \$222,000 award, and the Eighth Circuit rejected the defendant's argument that that lower award was unconstitutional. *Capitol Records, Inc. v. Thomas-Rasset*, 692 F.3d 899, 907–910 (8th Cir. 2012). To the extent that the district court's opinions remain authoritative, they are inapposite here because the case involved "a first-time willful, consumer infringer of limited means who committed illegal song file-sharing for her own personal use." *Thomas-Rasset II*, 799 F. Supp. 2d at 1001.

after bench trials or defaults have often awarded less than the jury did in this case, even where the infringing conduct could be characterized as more culpable. Def. Br. at 28–34. But the question is not what this Court would award were it deciding the question itself; the question is whether the jury’s award is so excessive that the Court should intrude on its prerogative to set damages. *See Feltner v. Columbia Pictures Television, Inc.*, 523 U.S. 340, 347–55 (1998) (recognizing the right to have a jury determine statutory damages); *Superior Form Builders, Inc. v. Dan Chase Taxidermy Supply Co.*, 74 F.3d 488, 496 (4th Cir. 1996) (jury’s award is entitled to significant deference); *Psihoyos I*, 2012 WL 5506121, at *1 (because remittitur involves usurping the jury’s authority to set damages, it is justified only in limited situations).

As noted, the Second Circuit has rejected the argument that statutory damages must have “a direct correlation” with actual damages. *Psihoyos II*, 748 F.3d at 127. The jury was entitled to consider other factors, including Defendants’ state of mind, a perceived need to deter Defendants and third parties, Defendants’ “cooperation in providing evidence concerning the value of the infringing material,” and the parties’ conduct and attitude. *See Bryant*, 603 F.3d at 144. There was evidence from which the jury could have concluded that Defendants’ infringement (and particularly AFP’s) was not just willful but reflected a gross disregard for the rights of copyright holders. In the light most favorable to Morel, AFP not only took Morel’s photographs from Twitter without pausing to consider whether it was infringing the copyright owner’s rights, but also continued selling the photographs (with an “AFP” identifier) even after learning of its infringement on the assumption that the only price to pay would be an after-the-fact payment close to what Morel would have earned had Defendants obeyed the law.

Additionally, although Defendants contend that the jury should not have considered deterrence as a meaningful factor in light of evidence that AFP and Getty “have each already

made changes to improve their systems and practices,” Def. Br. at 30, “an inclination on the part of the jury to impose a penalty to deter similar conduct in the future is not erroneous, notwithstanding the . . . revised policies, given the evidence of reckless conduct in the past.” *Psihoyos I*, 2012 WL 5506121, at *4. And as the Court held in addressing the parties’ motions in limine, it would have been appropriate for the jury to consider the fact that AFP and Getty are large companies in assessing deterrence. Final Pre-Trial Conf. Tr. at 21:9–19. It also would have been appropriate, under *Bryant*, to consider the deterrent effect on other potential infringers, which may not have changed their policies in the way that Defendants here claim to have done. *See Bryant*, 603 F.3d at 144; *Psihoyos I*, 2012 WL 5506121, at *4. In sum, the Court concludes that in light of all the considerations that the jury was entitled to consider, remittitur of the \$1.2 million statutory damages award is not required.

III. Conclusion

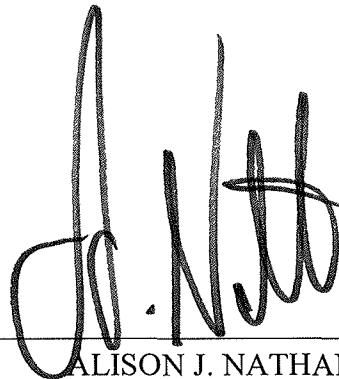
For the foregoing reasons, Defendants' motion for judgment as a matter of law, a new trial, and/or remittitur is GRANTED insofar as the Court grants judgment as a matter of law to Getty on Morel's claim under § 1202(b) of the DMCA. Accordingly, the jury's award is altered such that AFP and Getty continue to be jointly liable for \$1,210,000 and AFP is individually liable for the remaining \$10,000. The remainder of Defendants' motion is DENIED.

The parties have stipulated that the deadline for taxing costs and submitting any motions for attorneys' fees is fourteen days from the date of this order. Dkt. No. 311. The opposition and reply deadlines for any such motions will be governed by the Federal and Local Rules, unless the parties, within fourteen days, submit for the Court's approval a stipulation setting alternative deadlines.

This resolves Docket No. 313.

SO ORDERED.

Dated: August 13, 2014
New York, New York

A handwritten signature in black ink, appearing to read 'A. J. Nathan', is written over a horizontal line.

ALISON J. NATHAN
United States District Judge

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ILANA IMBER-GLUCK, on Behalf of Herself
and All Others Similarly Situated,

Plaintiff,

v.

GOOGLE, INC., a Delaware Corporation.

Defendant.

Case No. 5:14-CV-01070-RMW

**ORDER GRANTING IN PART AND
DENYING IN PART DEFENDANT
GOOGLE, INC.'S MOTION TO
DISMISS**

[Re: Docket No. 20]

Google, Inc. (“Google”), a Delaware corporation with its headquarters and principal place of business in California, is a leading seller of software applications (“Apps”) users can download onto their mobile computing devices. *See* Plaintiff’s Class Action Complaint (“Compl.”), Dkt. No. 1, ¶¶ 2-3. Plaintiff Ilana Imber-Gluck brings the instant class action complaint “on behalf of herself and other parents and guardians whose minor children: (a) downloaded from [Google] a free or modestly priced [App]; and (b) then incurred charges for in-game-related voidable purchases that the minor was induced by Google to make, without the parents’ and guardians’ knowledge or authorization.” *Id.* at ¶ 1.

Case No. 5:14-CV-01070-RMW

- 1 -

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT GOOGLE, INC.’S MOTION TO DISMISS

Pursuant to Federal Rule of Civil Procedure 12(b)(6), Google moves to dismiss plaintiff's class action complaint. Motion to Dismiss ("MTD"), Dkt. No. 20. The court GRANTS in part and DENIES in part Google's motion to dismiss.

I. FACTUAL AND PROCEDURAL BACKGROUND

Plaintiff alleges the following:

Google operates a digital distribution platform known as "Google Play" that permits users to browse and download applications developed for the Android operating system. Compl. ¶¶ 2-3. Apps, which are often games, are available through Google Play either free-of-charge or for a fee. *Id.* Many of these gaming Apps are designed to allow purchases of what Google refers to as "In-App Purchases" or "In-App Content," i.e., virtual supplies, cash, and content, which are designed to be used within the game itself ("Game Currency"). *Id.* at ¶ 3.

Prior to the purchase of content from Google Play, a user must establish a Google Play account. Compl. ¶ 18. Opening an account requires, among other things, creating a username and password, providing certain contact and personal information, and agreeing to Google's Terms of Service ("Terms of Service").¹ *Id.* In order to purchase content from Google Play, one typically supplies Google with a credit or debit card number or PayPal account through Google's "Google Wallet" function. *Id.* For each digital purchase, users who specify a credit, debit, or PayPal payment will have Google automatically draw funds from the account holder's specified credit or debit card or PayPal account. *Id.*

The purchase of an App or any Game Currency is a transaction completed directly between Google and the consumer. Compl. ¶ 17. Immediately prior to the purchase of content from Google Play, Google requires the account holder to enter her password. *Id.* at ¶ 19. Once the password is entered, the user is permitted to make subsequent purchases through her Google Play account for up to 30 minutes without reentering the password. *Id.*

In or around February 2012, plaintiff established a Google Play account utilizing her debit card and placed it on file to make future purchases of Google Play downloads and applications.

¹ The complaint refers to the Terms of Service as "Terms and Conditions." *See, e.g.*, Compl. ¶¶ 18, 38.

1 Compl. ¶10. In February 2014, plaintiff downloaded the App Marvel Run Jump Smash (“Run Jump
2 Smash”) onto her Samsung Galaxy Tab 2 10.1. *Id.* Within 30 minutes of permitting the download,
3 one of plaintiff’s minor sons made subsequent In-App Purchases of virtual content without
4 plaintiff’s authorization. *Id.* Plaintiff received an email notification that her Google Play account
5 had been charged \$65.95 for the purchased virtual content. *Id.*

6 On March 6, 2014, plaintiff filed a class action complaint, individually and on behalf of all
7 others similarly situated, seeking monetary, declaratory, and equitable relief under California’s
8 contract laws, Consumers Legal Remedies Act, Business and Professions Code § 17200, et seq.,
9 and/or for unjust enrichment. Compl. ¶ 5. The complaint asserts claims for: (1) declaratory
10 judgment pursuant to 28 U.S.C. § 2201, *et seq.*; (2) violation of the California Consumers Legal
11 Remedies Act; (3) violation of California’s Unfair Competition Law; (4) unjust
12 enrichment/restitution; and (5) breach of the duty of good faith and fair dealing. *See* Compl. In
13 response, Google filed the instant motion to dismiss. *See* MTD.

14 II. ANALYSIS

15 A. Motions to Dismiss and Leave to Amend

16 To survive a motion to dismiss pursuant to Rule 12(b)(6), a complaint must make “factual
17 allegations [that are sufficient] to raise a right to relief above a speculative level.” *Bell Atlantic*
18 *Corp. v. Twombly*, 550 U.S. 544, 555 (2007). On a motion to dismiss, a court must take all of the
19 factual allegations in a complaint as true, but the court need not accept as true “[t]hreadbare recitals
20 of the elements of a cause of action,” or legal conclusions presented as facts. *Ashcroft v. Iqbal*, 556
21 U.S. 662, 678 (2009). A trial court may also dismiss a claim *sua sponte* under Rule 12(b)(6) if it
22 determines a claimant clearly cannot win relief. *Omar v. Sea-Land Service, Inc.*, 813 F.2d 986, 991
23 (9th Cir. 1987).

24 When an allegation involves fraud pursuant to Rule 9(b), a heightened pleading standard
25 applies and a party must state with particularity the circumstances constituting fraud or mistake.
26 Fed. R. Civ. P. 9(b). A motion to dismiss a complaint or claim grounded in fraud under Rule 9(b)
27 for failure to plead with particularity is the functional equivalent of a motion to dismiss under Rule
28 12(b)(6) for failure to state a claim. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1107 (9th Cir.

2003). “If dismissal is granted under either Rule 12(b)(6) or 9(b), leave to amend should be allowed unless the pleading could not possibly be cured by the allegation of other facts.” *In re Apple In-App Purchase Litig.*, 855 F. Supp. 2d 1030, 1040 (N.D. Cal. 2012) (citing *Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir. 2000) and *Vess*, 317 F.3d at 1108).

B. Declaratory Judgment

Plaintiff seeks a declaratory judgment by this court pursuant to 28 U.S.C. § 2201, *et seq.* that:

(a) this action may proceed and be maintained as a class action; (b) the contracts between [d]efendant and the [c]lass members relating to the purchase of Game Currency are voidable at the option of the respective [c]lass members on behalf of their minor children; (c) if the [c]lass members elect to void the contracts, they will be entitled to restitution; (d) an award of reasonable attorneys’ fees and costs of suit to [p]laintiff and the [c]lass is appropriate; and (e) such other and further relief as is necessary and just may be appropriate as well.

Compl. ¶ 50. Plaintiff’s declaratory judgment claim rests on plaintiff’s allegations that each purchase of Game Currency is a contract between Google and minor children, which parents can disaffirm. Google moves to dismiss plaintiff’s declaratory judgment claim on two alternative grounds: (1) if the contracts are with plaintiff’s minor child, plaintiff does not have standing to disaffirm the contracts; and (2) that the contracts in question are with plaintiff and not plaintiff’s minor child.

1. Standing of Plaintiff to Disaffirm the Contracts of a Minor Child

Plaintiff alleges California Family Code § 6710 provides that the contract of a minor is voidable by disaffirmance by the minor or a parent or guardian on behalf of a minor. Compl. ¶¶ 46-49. Google argues that if any contracts were made with plaintiff’s minor child, as plaintiff alleges, this claim should be dismissed as a matter of law because plaintiff does not have standing to disaffirm the contracts of her minor child as she did not sue on behalf of her minor child. MTD 3-5.

Plaintiff acknowledges that under California Family Code § 6710, the contract of a minor may only be disaffirmed by the minor, but argues that § 6710 only refers to which party in the transaction can disaffirm, averring “it would be untenable to require the minors (some younger than

four years old) to knowingly express disaffirmance.” MTD 6-7 (citing *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1036 n.4). However, plaintiff is incorrect in both her assumption that § 6710 requires the minor to “knowingly express disaffirmance” and that such a requirement would undermine the utility of § 6710. *Id.* at 7. As Google points out, express disaffirmance by the minor himself or herself is not required because a legal representative of the minor may bring the case on the minor’s behalf. Google, Inc.’s Reply in Support of MTD (“Reply”), Dkt. No. 24, at 1.

The power to disaffirm a minor’s contract does not extend to the minor’s parents. *See I.B. ex rel. Fife v. Facebook, Inc.*, 905 F. Supp. 2d 989, 1004-05 (N.D. Cal. 2012) (dismissing the claims of plaintiffs who did not bring their claims on behalf of their minor children). Because plaintiff did not bring suit on behalf of her minor child, she does not have standing to disaffirm any contracts made by her minor child.

2. Contracts between Google and Minor Child

Plaintiff has sufficiently alleged that each In-App Purchase constituted a contract with her minor son. Plaintiff’s theory is that Google made an offer, in the form of all Game Currency Google presented for sale. Compl. ¶ 42. Plaintiff’s minor son accepted that offer through his purchase of Game Currency from Google. *Id.* at ¶ 43.

Google argues that plaintiff’s declaratory judgment claim should be dismissed as a matter of law because all purchases made on the plaintiff’s account are governed by the Terms of Service, a contract between Google and Plaintiff. MTD 5-6. If, as Google argues, the contract is not with a minor, then the contract is not voidable under California Family Code § 6710. Google further contends that, as all purchases were “made through [p]laintiff’s device, using [p]laintiff’s Google Play account, and were billed to [p]laintiff,” the Terms of Service control, which make plaintiff responsible for all transactions on her account. *Id.* at 5; *see also* Schmidtlein Decl. Ex. B (Dkt. No. 20-1), at 2.

Plaintiff responds that the Terms of Service do not control because the contracts at issue are the individual purchases of Game Currency by the minor, not the creation of plaintiff’s Google Play account. Plaintiff’s Opposition to MTD (“Opp.”), Dkt. No. 23, at 4. Plaintiff argues that even if the

1 Terms of Service do control the contracts, the terms are ambiguous and thus subject to
2 interpretation. *Id.* at 5.

3 Under California law, “courts may not dismiss on the pleadings when one party claims that
4 extrinsic evidence renders the contract ambiguous. The case must proceed beyond the pleadings so
5 that the court may consider the evidence.” *A. Kemp Fisheries, Inc. v. Castle & Cooke, Inc.*, 852 F.2d
6 493, 497 n.2 (9th Cir. 1988). However, if “the court decides that the contract is not reasonably
7 susceptible to more than one interpretation, the court can reject the assertion of ambiguity.” *Skilstaf,*
8 *Inc. v. CVS Caremark Corp.*, 669 F.3d 1005, 1115 (9th Cir. 2012).

9 Plaintiff alleges that the term “authorized” is ambiguous and seeks to introduce extrinsic
10 evidence as to whether the Terms of Service apply to contracts generated from unauthorized use of
11 accounts. *Id.* Google counters that no extrinsic evidence is required to determine that the Terms of
12 Service define the contract as between the plaintiff and Google. *See* Reply 4. Moreover, the term
13 “authorized” does not appear in the relevant sections of the Terms of Service, and plaintiff does not
14 allege that any other terms in the Terms of Service are ambiguous.

15 In sum, plaintiff’s pleading is deficient in two regards. If the alleged contracts at issue are
16 between plaintiff’s minor child and Google, then plaintiff does not have standing to void the
17 contracts on behalf of her child. She would have to sue in a representative capacity. If the contracts
18 are instead between plaintiff and Google, plaintiff has not alleged any terms actually present in the
19 Terms of Service which might render the Terms of Service ambiguous or suggest that plaintiff is not
20 liable for the allegedly unauthorized purchases by her minor sons. Therefore, the court GRANTS
21 Google’s motion to dismiss plaintiff’s declaratory judgment claim, with leave to amend.

22 **C. CLRA Claim**

23 Plaintiff alleges Google violated the Consumers Legal Remedies Act (“CLRA”) by
24 concealing the ability to use real-world currency to purchase Game Currency in gaming Apps
25 labelled as “free,” with the intent of inducing minors to purchase said Game Currency. Compl. ¶ 54.
26 In so doing, plaintiff alleges Google has violated: (1) Cal. Civ. Code § 1770(a)(5), by “representing
27 that goods or services have sponsorship, approval, *characteristics*, ingredients, *uses*, benefits, or
28 qualities that they do not have”; (2) Cal. Civ. Code § 1770(a)(7), by “representing that goods or

1 services are of a particular *standard, quality*, or grade . . . if they are of another”; and (3) Cal. Civ.
2 Code § 1770(a)(14), by “representing that a transaction confers or involves rights, remedies, or
3 obligations which it does not have or involve, or which are prohibited by law.” Cal. Civ. Code
4 § 1770 (emphasis added); *see also* Compl. ¶ 54. Plaintiff further alleges Google had a duty to
5 disclose material facts about the Game Currency offered in Apps it “marketed, advertised, and
6 promoted to children as ‘free.’” *Id.* at ¶ 56.

7 Google argues plaintiff’s CLRA claim is procedurally defective due to a failure to fulfill the
8 heightened pleading requirements of Rule 9(b), which require that “in allegations of fraud or
9 mistake, a party must state with particularity the circumstances constituting fraud or mistake” and
10 that “[m]alice, intent, knowledge, and other conditions of a person’s mind may be alleged
11 generally.” MTD 11; *see also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009)
12 (stating that Rule 9(b) always applies to claims of violation of the CLRA). Plaintiff argues that she
13 has sufficiently alleged CLRA claims under Rule 9(b). Opp. 11.

14 A duty to disclose arises under the CLRA in four cases: “(1) when the defendant is in a
15 fiduciary relationship with the plaintiff; (2) when the defendant has the exclusive knowledge of
16 material facts not known to the plaintiff; (3) when the defendant actively conceals a material fact
17 from the plaintiff; and (4) when the defendant makes partial representations but also suppresses
18 some material fact.” *Wilson v. Hewlett-Packard Co.*, 668 F.3d 1136, 1142 (9th Cir. 2012) (quoting
19 *Falk v. General Motors Corp.*, 496 F. Supp. 2d 1088, 1095 (N.D. Cal. 2007)). A non-disclosed fact
20 is material when the plaintiff can show that, had the fact been disclosed, the plaintiff would have
21 been “aware of it and behaved differently.” *Id.* (quoting *Mirkin v. Wasserman*, 5 Cal. 4th 1082, 1093
22 (1997)).

23 Plaintiff has sufficiently alleged that Google had a duty to disclose material facts about the
24 Game Currency in the “games it marketed, advertised, and promoted to children as ‘free.’” Compl.
25 ¶ 56. Plaintiff has further specifically alleged the misrepresentations she was exposed to and the
26 resulting harm. Plaintiff pled specific facts that Google “actively advertis[ed], market[ed], and
27 promot[ed] certain gaming Apps as ‘free.’” *Id.* at ¶ 69. Plaintiff has also alleged she was charged
28 money after Game Currency was purchased without her authorization. *Id.* at ¶ 10.

1 Google argues plaintiff has not sufficiently alleged a claim for relief because “she fails to
2 identify a single game that she downloaded that was ‘free.’” MTD 12. In support, Google argues
3 Run Jump Smash costs \$0.99, attaching a printout of the Google Play page for the App. *See*
4 Schmidlein Decl. Ex. A (Dkt. No. 20-1). However, as plaintiff correctly points out, a district court
5 generally “may not consider any material beyond the pleadings in ruling on a 12(b)(6) motion to
6 dismiss for failure to state a claim.” *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001).

7 Nonetheless, plaintiff alleges she downloaded Run Jump Smash and “[i]n the 30 minutes
8 after [she] permitted the download, a subsequent purchase was made in the Run Jump Smash game
9 without her authorization.” Compl. ¶ 10. Plaintiff further alleges she “was given no indication by
10 Google that [she was] approving anything more than a single ninety-nine-cent (\$0.99) transaction.”
11 *Id.* at ¶ 26. Because plaintiff did not authorize a purchase after the download, but did authorize a
12 \$0.99 purchase as part of the transaction, her allegation only makes sense if the purchase of the App
13 was for \$0.99. Additionally, plaintiff argues her usage of the term “free” was merely for brevity, and
14 that a nominal cost, in all cases \$0.99, was included in the term. Opp. 12.

15 The parties’ dispute over the price of the App notwithstanding, it is clear from the complaint
16 as a whole that “free” includes both free and nominally valued App purchases, such as those that
17 cost \$0.99. *See, e.g.*, Compl. ¶ 1 (“free or moderately priced application”); *Id.* at ¶ 22 (“free or cost
18 a nominal charge”); *Id.* at ¶ 28 (“free or inexpensive (e.g. \$0.99)”). Plaintiff sufficiently alleges that
19 she purchased a free or nominally priced App. *See id.* at ¶ 10 (alleging plaintiff downloaded Run
20 Jump Smash); *id.* at ¶ 26 (alleging plaintiff was given no indication she was approving more than
21 \$0.99).

22 However, plaintiff has failed to sufficiently allege that she relied upon Google’s
23 misrepresentation or that she would have behaved differently had she been aware of it. While
24 plaintiff alleges she was charged \$65.95 without her authorization and that Google gave her no
25 indication that she was approving anything more than a \$0.99 purchase, she fails to explicitly allege
26 that she was unaware of either the 30-minute password duration or the ability to make In-App
27 Purchases. Compl. ¶¶ 10, 26.

1 Plaintiff has also not sufficiently alleged materiality because she has not alleged that she
2 would have acted differently, had she been aware of the ability to make purchases without
3 reentering her password. It seems clear from plaintiff's complaint and opposition to the motion to
4 dismiss that plaintiff could allege facts sufficient to show reliance and materiality. Therefore, the
5 court GRANTS Google's motion to dismiss plaintiff's CLRA claim, with leave to amend.

6 **D. Unfair Competition Law Claim**

7 Plaintiff alleges Google violated California's Unfair Competition Law, Business &
8 Professions Code § 17200, *et seq.* ("UCL"), through "unlawful," "unfair," and "fraudulent" business
9 acts or practices and "unfair, deceptive or misleading" advertising. Compl. ¶¶ 62-74. The UCL
10 "prohibits acts of 'unfair competition' defined as: (1) unlawful business acts or practices; (2) unfair
11 business acts or practices; (3) fraudulent business acts or practices; and (4) unfair, deceptive or
12 misleading advertising." *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1040. Rule 9(b)'s
13 heightened pleading requirements apply to UCL "unfair" and "unlawful" business act or practice
14 claims which are dependent upon allegations of fraudulent omissions and misrepresentations. *Id.* at
15 1039; *see also Kearns.*, 567 F.3d at 1126-27; *In re Facebook PPC Adver. Litig.*, 2010 WL 3341062,
16 at *9 (N.D. Cal. Aug. 25, 2010).

17 Here, plaintiff's "unfair" and "unlawful" business practice claims are dependent upon
18 allegations that Google made fraudulent misrepresentations and omissions regarding Google's free
19 and nominally priced Apps, and therefore Rule 9(b)'s pleading requirements apply.

20 **1. Unlawful Business Acts or Practices**

21 A business's violations of law are actionable "unlawful" business acts or practices under the
22 UCL. *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1040 n. 7 (citing *In re Actimmune*
23 *Marketing Litig.*, 2009 WL 3740648, at *15 (N.D. Cal. Nov. 6, 2009)). To state a claim for unlawful
24 business acts or practices under the UCL, "it is not necessary that plaintiffs allege violation of the
25 predicate laws with particularity; they must at a minimum, however, identify the statutory or
26 regulatory provisions that defendants allegedly violated." *Id.* (quoting *Actimmune*, 2009 WL
27 3740648, at *15).

Plaintiff alleges Google committed an unlawful business act or practice in violation of the UCL when Google violated the CLRA. Compl. ¶ 68. Plaintiff does not allege any other statutory violation by Google as predicate to a claim for unlawful business acts or practices under the UCL. As previously discussed in the analysis of plaintiff's CLRA claim, plaintiff has not sufficiently alleged that Google has committed a CLRA violation. Because plaintiff has not sufficiently identified a statutory or regulatory provision that Google allegedly violated, plaintiff has failed to state a claim for "unlawful" business acts or practices under the UCL.

2. Unfair Business Acts or Practices

Under the UCL, "[a business] act or practice is unfair if the consumer injury is substantial, is not outweighed by any countervailing benefit to consumers or to competition, and is not an injury the consumers themselves could reasonably have avoided." *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1040 (quoting *Tietsworth v. Sears, Roebuck and Co.*, 2009 WL 3320486, at *7 (N.D. Cal. Oct. 13, 2009)). For the purpose of alleging an "unfair" business act or practice, demonstrating "aggregate harm on consumers is sufficient to show substantial injury." *F.T.C. v. Inc21.com Corp.*, 688 F. Supp. 2d 927, 939 (N.D. Cal. 2010).

Plaintiff alleges she and class have suffered substantial harm in the aggregate by incurring Google Play charges that they did not explicitly authorize. Compl. ¶¶ 10, 72. Plaintiff also contends she could not have reasonably avoided the injury as she "was given no indication by Google that [she] was approving anything more than a single ninety-nine cent (\$0.99) transaction" and that she was deceived by Google's practices. *Id.* at ¶¶ 26, 71. However, plaintiff does not allege that the harm of Google's purported unfair business act outweighs any countervailing benefit to consumers or to competition. Therefore, plaintiff has failed to sufficiently allege that Google has committed an "unfair" business practice or act under the UCL.

3. Fraudulent Business Acts or Practices

To state a claim for "fraudulent" business acts or practices under the UCL, "plaintiffs must allege with specificity that defendant's alleged misrepresentations: (1) were relied upon by the named plaintiffs; (2) were material; (3) influenced the named plaintiffs' decision to purchase the product; and (4) were likely to deceive members of the public." *Apple In-App Purchase Litig.*, 855

1 F. Supp. 2d at 1041 (citing *Tietsworth*, 2009 WL3320486, at *8). The sufficiency of a plaintiff's
2 UCL fraud claim may be analyzed together with the plaintiff's CLRA claim. *Id.* (citing *Kowalsky v.*
3 *Hewlett-Packard Co.*, 2011 WL 3501715 (N.D. Cal. Aug. 10, 2011)).

4 As discussed above, plaintiff has not pled specific facts to support a claim for violation of
5 the CLRA. Plaintiff has alleged that Google's business acts or practices were likely to deceive the
6 public. Compl. ¶¶ 69, 71. However, plaintiff has failed to allege Google's misrepresentations were
7 relied upon by plaintiff, were material, and influenced plaintiff's decision to purchase the product.
8 Therefore, plaintiff has failed to sufficiently allege that Google has committed "fraudulent" business
9 acts or practices under the UCL.

10 **4. Unfair, Deceptive or Misleading Advertising**

11 To state a claim for "unfair, deceptive or misleading" advertising under the UCL, "a plaintiff
12 need merely allege that members of the public are likely to be deceived by defendants' conduct."
13 *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1040 n. 10 (quoting *Actimmune*, 2009 WL
14 3740648, at *7).

15 Plaintiff alleges Google actively advertised, marketed and promoted certain gaming Apps as
16 "free" with the intent to lure minors to purchase Game Currency in a manner likely to deceive the
17 public. Compl. ¶ 69. Plaintiff alleges Google's deceptive practices have deceived and/or are likely
18 to deceive members of the public. *Id.* at ¶ 71. Plaintiff has sufficiently alleged that Google has
19 committed "unfair, deceptive or misleading" advertising under the UCL.

20 In sum, taking all factual allegations in the complaint as true, plaintiff has sufficiently pled a
21 claim for "unfair competition" under the UCL through "unfair, deceptive or misleading"
22 advertising. Plaintiff has failed to plead claims for "unfair competition" under the UCL through
23 allegations of violations of "unlawful," "unfair," and "fraudulent" business acts or practices.

24 The court GRANTS Google's motion to dismiss Plaintiff's UCL claim for violations of
25 "unlawful," "unfair," and "fraudulent" business acts or practices with leave to amend. The court
26 DENIES Google's motion to dismiss plaintiff's UCL claim for violations of "unfair, deceptive or
27 misleading" advertising.

E. Unjust Enrichment and Restitution

Plaintiff alleges that Google has been unjustly enriched at the expense of plaintiff and class by collecting money Google is not entitled to. Compl. ¶ 79. Plaintiff further alleges that she and the class are entitled to recover from Google all amounts wrongfully collected and improperly retained by Google, plus interest. *Id.* at ¶ 80.

Google argues that the Ninth Circuit has held that “unjust enrichment ‘does not describe a theory of recovery’ under California law.” MTD 7 (quoting *In re Sony PS3 “Other OS” Litigation*, 551 F. App’x 916, 923 (9th Cir. 2014)). Rather than a theory of recovery, Google argues that unjust enrichment is a principle “underlying various legal doctrines and remedies.” *Id.* (citing *Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 932 (N.D. Cal. 2012)).

Plaintiff argues in response that recent Ninth Circuit precedent runs contrary to Google’s argument. Opp. 7. The most recent Ninth Circuit decision on the subject incorporates unjust enrichment as an independent claim. *See Berger v. Home Depot USA, Inc.*, 741 F.3d 1061, 1070 (9th Cir. 2014) (providing the elements of unjust enrichment as the “receipt of a benefit and unjust retention of the benefit at the expense of another”) (quoting *Lectrodryer v. SeoulBank*, 77 Cal. App. 4th 723, 726 (Cal. Ct. App. 2000); *see also Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1042 (permitting a claim for unjust enrichment under similar circumstances); *Ellsworth v. U.S. Bank, N.A.*, 908 F. Supp. 2d 1063, 1088 (N.D. Cal. 2012) (holding plaintiff could proceed with unjust enrichment claim at the motion to dismiss stage).

Google’s argument that the court should ignore *Berger* is unpersuasive. Reply 7. While Google is correct that the issue in that case was class certification, the Ninth Circuit first discussed unjust enrichment as a claim before determining that the plaintiff’s claim for unjust enrichment was not susceptible to class treatment in that specific case. *Berger*, 741 F.3d at 1070. Other recent cases also point to unjust enrichment as a cause of action in California. *See Gabriel v. Alaska Elec. Pension Fund*, No. 12-35458, 2014 WL 2535469, at *8 (9th Cir. June 6, 2014) (noting that “the remedy of surcharge is available against the fiduciary ‘for benefits it gained through unjust enrichment’” (quoting *Skinner v. Northrop Grumman Retirement Plan B*, 673 F.3d 1162, 1167 (9th Cir. 2012)) ; *E.J. Franks Construction, Inc. v. Sohota*, F066327, 2014 WL 2526978, at *1 (Cal. Ct. Case No. 5:14-CV-01070-RMW

App. June 5, 2014) (allowing plaintiff to bring unjust enrichment claims to trial); *People v. Sarpas*, 255 Cal. Rptr. 3d 25, 47 (2014) (holding “plaintiffs had ‘stated a valid cause of action for unjust enrichment’” (quoting *Hirsch v. Bank of America*, 107 Cal. App. 4th 708, 722 (2003))).

Google’s suggestion that the court follow an unpublished, non-precedential report is similarly unpersuasive. Even permitting that *Berger* did not expressly hold that California law recognizes an unjust enrichment cause of action, the factually analogous *In re Apple In-App Purchase Litigation* allowed the plaintiffs to proceed with an unjust enrichment claim at the motion to dismiss stage. *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1042. Therefore, the court DENIES Google’s motion to dismiss plaintiff’s claim for unjust enrichment.

F. Breach of Duty of Good Faith and Fair Dealing

Plaintiff alleges Google breached its contractual duty of good faith and fair dealing with plaintiff and class. Compl. ¶¶ 82-89. Plaintiff specifically alleges Google engaged in conduct apart from its agreement² with plaintiff and class, without good faith, “for the purpose of depriving plaintiff and . . . class of rights and benefits under the contract, to wit, a sales transaction for an item the consumer *intended* to purchase.” *Id.* at ¶¶ 85, 87 (emphasis in original). Google argues plaintiff’s claim fails as a matter of law because under California law the implied covenant cannot be used to negate an express term of the parties’ contract to which plaintiff agreed. MTD 9-10. Google also argues plaintiff’s claim fails because the implied covenant cannot be used to impose additional terms and duties to a contract – i.e. imposing that a consumer’s “inten[t] to purchase” is a condition precedent to engaging in an enforceable sales transaction with Google. *Id.* at 10-11

Every contract in the state of California contains an implied covenant of good faith and fair dealing that neither party will injure the right of the other party to receive the benefits of the agreement. *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1041 (citing *Wolf v. Walt Disney Pictures & Tel.*, 162 Cal. App. 4th 1107, 1120 (2008)). The covenant is implied in every contract in order to protect the express covenants or promises of the contract. *Id.* at 1041-42 (citing *Carma Developers (Cal.), Inc. v. Marathon Development California, Inc.*, 2 Cal. 4th 342, 373 (1992)). The

² “Agreement” refers to the Terms of Service to which each member of the class agreed when they opened a Google Play account.

covenant will not be implied “to prohibit a party from doing that which is expressly permitted by the agreement itself.” *Id.* at 1042 (citing *Carma*, 2 Cal. 4th at 373). The implied covenant “cannot impose substantive duties or limits on the contracting parties beyond those incorporated in the specific terms of their agreement.” *Appling v. State Farm Mut. Auto. Ins. Co.*, 340 F.3d 769, 779 (9th Cir. 2003) (quoting *Guz v. Bechtel Nat. Inc.*, 24 Cal. 4th 317, 350 (2000)). “To establish a claim for breach of the implied covenant of good faith and fair dealing, [p]laintiffs must show that [defendant] lacked subjective good faith in the validity of its act or the act was intended to and did frustrate the common purpose of the agreement.” *Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1042 (citing *Carma*, 2 Cal. 4th at 373).

Here, Google’s Terms of Service signed by plaintiff and class expressly provides that signees are “responsible for the activity that happens on or through [their] Google account[s].” Schmidlein Decl. Ex. B (Dkt. No. 20-1) at 2. This express provision agreed to by plaintiff and class entitles Google to bill plaintiff and class’s Google Play accounts for charges incurred through such activity regardless of their intent. However, plaintiff has alleged that Google encouraged children to make In-App Purchases, without providing notice to the parent or guardian of the 30-minute window in which the account holder’s password is not required to make subsequent purchases. Compl. ¶ 29. Such acts may frustrate the common purpose of the agreement by forcing parents to pay for purchases that Google induced parents’ minor children to make.

Therefore, plaintiff has sufficiently pled facts which would demonstrate how Google breached the duty of good faith and fair dealing. Accordingly, the court DENIES Google’s motion to dismiss plaintiff’s claim for breach of the implied covenant of good faith and dealing.

III. ORDER

For the reasons explained above, the court orders as follows with respect to each of the claims at issue:

- Declaratory Judgment: Dismissed with 30 days leave to amend.
- CLRA: Dismissed with 30 days leave to amend.

- 1 • UCL
 - 2 ○ Unlawful business practices or act: dismissed with 30 days leave to amend.
 - 3 ○ Unfair business practices or act: dismissed with 30 days leave to amend.
 - 4 ○ Fraudulent business acts: dismissed with 30 days leave to amend.
 - 5 ○ Unfair, deceptive or misleading advertising: not dismissed.
- 6 • Unjust Enrichment and Restitution: Not dismissed.
- 7 • Breach of Good Faith and Fair Dealing: Not dismissed.

8 Dated: July 21, 2014


Ronald M. Whyte
United States District Judge