Chapter 17

Data Breach Litigation Involving Consumer Class Actions

Margaret A. Dale & David A. Munkittrick

Proskauer Rose LLP

§ 17:1 Introduction

While consumer class action litigation following a data breach now seems routine, with lawsuits filed after every major and not-so-major

report of a breach, the jurisprudence in the area is actually only about ten years old. And while a data breach can be perpetrated in any number of ways, the legal issues that arise from the theft or loss of data largely fall within the same set of legal paradigms. The focus of this chapter is to survey the development of the law in the area of consumer class action litigation.

§ 17:2 Consumer Plaintiff Theories of Liability

§ 17:2.1 Causes of Action

As can be expected in a developing area like data breach litigation, plaintiffs' liability theories span a range of federal and state statutory and common law claims. Of course, each theory is premised on unauthorized access to personal information and the alleged harm of identity theft or the increased risk of identity theft. There are staple causes of action: negligence, breach of contract, fraud, violation of consumer protection statutes, violation of the Stored Communications Act (SCA),[1] breach of fiduciary duty, and invasion of privacy, among others. The following subsections review some of the nuances of these theories specific to the data breach context.

[A] Negligence

Almost every data breach case includes a common law claim for negligence. Negligence claims require a standard set of elements: a duty to exercise reasonable care, and a failure to exercise that care, which caused actual damage.[2] To establish a duty of care in a data breach case, plaintiffs often point—not always successfully—to alleged promises made by defendants regarding data security or to industry-specific security protocols.[3] A duty of care can also be established by statute. For instance, the Gramm-Leach-Bliley Act has been found to impose a duty on financial institutions to protect the security and confidentiality of customers' nonpublic personal information.[4]

---

1. *See supra* chapter 6 (for a more complete discussion of the SCA).
2. *See, e.g.*, Willingham v. Glob. Payments, Inc., 2013 WL 440702 (N.D. Ga. 2013); Irwin v. RBS Worldpay, Inc., 2010 U.S. Dist. LEXIS 145301 (N.D. Ga. 2010); McLoughlin v. People's United Bank, Inc., 2009 WL 2843269 (D. Conn. 2009); Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., 2009 WL 799760 (E.D. La. 2009); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009); Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307 (S.D.N.Y. 2008).
3. *See, e.g.*, *Willingham*, 2013 WL 440702, at *18; *In re* Michaels Stores Pin Pad Litig., 830 F. Supp. 2d 518, 528 (N.D. Ill. 2011) (PIN pad security requirements); *see also* chapter 16, *supra* (for more on such security standards).
4. *See* Guin v. Brazos Higher Educ. Serv. Corp., 2006 WL 288483, at *3 (D. Minn. Feb. 7, 2006).

[B] Breach of Contract

Breach of contract theories are probably the second most common theories alleged. A contractual relationship in the data breach context can arise from a retail transaction, such as the acceptance of credit or debit card for payment in exchange for goods or services.[5] A company's privacy policy can also be the basis for a breach of contract claim by its customers.[6]

[C] Fraud

Fraud allegations usually involve a claim that a defendant misrepresented the state of its data security or fraudulently concealed a data breach.[7] Such claims are brought under common law fraud theories or at times under state consumer protection laws.[8]

§ 17:2.2 Actual Damages

The common law theories of liability, such as negligence, breach of contract, and fraud, all require actual damages.[9] As discussed in more detail below, plaintiffs often fail this element at the pleading stage.

§ 17:3 Defense Strategies

Just as plaintiffs' theories of liability continue to evolve in response to the growing volume of reported data breach decisions (still mostly on motions to dismiss), so too do defense strategies. The mainstay defense continues to be Article III standing, challenging whether plaintiffs have adequately alleged an injury in fact, a causal relationship between the alleged conduct and the injury, and a likelihood that

---

5. *See* Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775, 780 (W.D. Mich. 2006); *Michaels Stores*, 830 F. Supp. 2d at 531 (finding sufficient allegations of an implied contract with customers to "take reasonable measures to protect the customers' financial information").
6. *See* Yunker v. Pandora Media, Inc., 2014 WL 988833, at *5 (N.D. Cal. Mar. 10, 2014). Plaintiffs have also couched their contract claims in terms of implied contract. *See* Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *1 (E.D. La. July 14, 2014). An implied contract is formed where the parties' conduct is assumed to have created an enforceable agreement. Order, Irwin v. RBS Worldpay, Inc., No. 1:09-CV-0033-CAP, 2010 U.S. Dist. LEXIS 145301, at *20–21 (N.D. Ga. Feb. 5, 2010).
7. *See* Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307, at *11 (S.D.N.Y. June 25, 2010); *see also infra* section 17:3.1[C] (discussing *Hammond*).
8. *See, e.g.*, *Michaels Stores*, 830 F. Supp. 2d at 529.
9. *See, e.g.*, Belle Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., No. 08-1568, 2009 WL 799760 (E.D. La. Mar. 24, 2009), at *1; *Hammond*, 2010 WL 2643307, at *2 (an element of breach of contract is resulting damage).

a favorable ruling will redress the injury. Decisions on standing in the data breach context now proliferate, though there remain distinctions among the circuits. The discussion that follows surveys the current, controlling Supreme Court and circuit court positions, as well as representative district court opinions.

§ 17:3.1 *Standing*

[A] The Supreme Court on Standing: *Clapper* and *Driehaus*

Most data breach litigation is based on an allegation of future harm—that the data breach put plaintiffs at greater risk of future identity theft. Though not a data breach case, the Supreme Court's seminal 2013 decision in *Clapper* addressed future harm and the standing doctrine.[10] In *Clapper*, plaintiffs challenged the constitutionality of 2008 amendments to the Foreign Intelligence Surveillance Act (FISA) that empowered the Foreign Intelligence Surveillance Court to authorize surveillance of persons reasonably believed to be outside the United States.[11] Plaintiffs, U.S. citizens and organizations, alleged that their international communications would likely be acquired under such surveillance in the future.[12] The Supreme Court found that such an allegation of future injury was too speculative because it relied on assumptions that the government would decide to target persons with whom plaintiffs communicate, that the government would invoke FISA to do so, that the government will succeed in intercepting such communications, and that the plaintiffs will be parties to the particular communications intercepted.[13] This did not satisfy the requirement of "certainly impending" harm required for standing.[14]

The *Clapper* plaintiffs also alleged that they suffered present injury in the form of costly and burdensome measures to protect the confidentiality of their international communications.[15] But the Supreme Court found this insufficient to confer standing: "[R]espondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[16] Both of these holdings, as to present and future injury, have found direct application in data breach cases.

---

10. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).
11. *Id.* at 1150; *see also* chapter 7, *supra* (for further discussion of intelligence gathering under FISA).
12. *Id.* at 1143.
13. *Id.* at 1148.
14. *Id.* at 1143.
15. *Id.*
16. *Id.*

A third aspect of *Clapper* is relevant in the data breach context. To establish Article III standing, an injury must, in addition to being "concrete, particularized, and actual or imminent," be "fairly traceable to the challenged action."[17] The speculative chain required to reach an actual, imminent injury also meant the challenged conduct in *Clapper* could not be fairly traced to such injury absent speculation.[18]

A second Supreme Court decision has also seen play in the data breach context, though it is not a data breach case either. In *Susan B. Anthony List v. Driehaus*, plaintiffs brought a pre-enforcement challenge to an Ohio statute that prohibited certain false statements during the course of a political campaign.[19] Again, the issue of future harm was front and center. The plaintiffs alleged that they intended future dissemination of information criticizing votes relating to the Patient Protection and Affordable Care Act.[20] The district court had dismissed the suit on the ground that it did not present a sufficiently concrete injury to meet standing or ripeness requirements, and the Sixth Circuit affirmed. However, the Supreme Court reversed,[21] finding the threat of future enforcement was substantial given the history of past enforcement and that such enforcement proceedings were not rare.[22]

[B] Data Breach Standing in Circuit Courts of Appeals

While the Supreme Court has not had occasion to hear a data breach case, at least four of the circuits have. Soon after *Clapper*, it appeared the decision may have signaled the death knell of private data breach litigation because very few data breach plaintiffs could actually show "certainly impending" injury.[23]

---

17. *Id.* at 1140–41 (citing Monsanto Co. v. Geertson Seed Farms, 561 U.S. 129 (2010)).
18. *Id.* at 1148–50.
19. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334 (2014).
20. *Id.* at 2339.
21. Susan B. Anthony List v. Driehaus, 805 F. Supp. 2d 412 (S.D. Ohio 2011), *aff'd*, 525 F. App'x 415 (6th Cir. 2013), *cert. granted*, 134 S. Ct. 2334, *rev'd and remanded*, 574 F. App'x 597 (2014).
22. *Id.*, 134 S. Ct. at 2345–46.
23. *See, e.g.*, Polanco v. Omnicell, Inc., 988 F. Supp. 2d 451, 466 (D.N.J. 2013) (dismissing putative class action for lack of standing where there was no allegation the information was actually read, reviewed, understood, or misused, leading the court to find *Clapper*'s "certainly impending" standard was not met); *In re* Barnes & Noble Pin Pad, 2013 U.S. Dist. LEXIS 125730, at *8 (N.D. Ill. Sept. 3, 2013) (dismissing for lack of standing in the absence of any allegation of the required "certainly impending" injury, notwithstanding an allegation of actual fraudulent charges to one of plaintiff's credit cards because there was no allegation that the plaintiff was not reimbursed or otherwise suffered actual harm as a result).

But in July 2015, the first federal appellate court to apply *Clapper* to a data breach case found the plaintiffs had sufficiently alleged injury to confer standing.[24] In 2013, hackers stole customer credit card numbers from a Neiman Marcus database, and several customers brought a class action seeking various forms of relief. The district court dismissed for lack of standing, but the Seventh Circuit reversed.[25] The plaintiffs pointed to six general types of injury:

(1) lost time and money resolving fraudulent charges;

(2) lost time and money protecting themselves from future identity theft;

(3) financial loss of buying items at Neiman Marcus that they would not have purchased if they had known of the store's cybersecurity vulnerabilities;

(4) lost control over the value of their personal information;

(5) increased risk of future fraudulent charges; and

(6) greater susceptibility to identity theft.[26]

The latter two constituted allegations of future harm.

Citing the Northern District of California's decision in *In re Adobe Systems, Inc. Privacy Litigation*, the Seventh Circuit found the plaintiffs had adequately alleged a certainly impending injury.[27] Allegations that the hackers specifically targeted Neiman Marcus and that the plaintiffs' credit card information had actually been stolen left an "objectively reasonable likelihood" that identity theft would occur in the future.[28] The court found the plaintiffs need not wait for the threatened harm to actually occur.

As revealed by the Seventh Circuit's citation of *Adobe Systems*, the Ninth Circuit is largely in line with the Seventh Circuit. In a pre-*Clapper* decision, it found standing in a case where data was stolen but there was no actual identity theft.[29] In *Krottner v. Starbucks*, plaintiff employees were found to have standing where a laptop with employee information was stolen. The threat of future identity theft, the court

---

24. Remijas v. Neiman Marcus Grp. LLC, 794 F.3d 688, 694 (7th Cir. 2015).
25. Remijas v. Neiman Marcus Grp. LLC, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014), *rev'd and remanded*, 794 F.3d 688 (7th Cir. 2014).
26. *Id.*, 794 F.3d at 692, 694.
27. *Id.* at 693 (citing *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1214 (N.D. Cal. 2014)).
28. *Id.* (quoting *Clapper*, 133 S. Ct. at 1147).
29. Krottner v. Starbucks, 628 F.3d 1139, 1142 (9th Cir. 2010).

found, was "credible," "both real and immediate," and "not conjectural or hypothetical."[30] This satisfied Article III.[31]

Not all circuits have reached the same result. The Third Circuit, in *Reilly v. Ceridian Corp.*, affirmed the district court's ruling that the allegations of injury were too speculative to establish standing.[32] In that case, the defendant suffered a security breach in 2009 when an unknown hacker potentially gained access to personal and financial information of approximately 27,000 people. The plaintiffs asserted claims of negligence and breach of contract. The court reasoned that any future injury relied on conjecture that the hacker:

(i) read, copied, and understood the plaintiffs' personal information;

(ii) intended to use the information for future crimes; and

(iii) could use the information to the plaintiffs' detriment.

For the Third Circuit, "unless and until these conjectures come true, [plaintiffs] have not suffered any injury."[33]

In another pre-*Clapper* decision, the Eleventh Circuit, in *Resnick v. AvMed, Inc.*, considered a case that included allegations of actual identity theft as well as future harm.[34] It held the plaintiffs had standing to sue a health insurance company after a company laptop with unencrypted data was stolen and the plaintiffs were subsequently victims of identity theft. In addition to finding the alleged injury (identity theft) was fairly traceable to defendant's conduct, the *Resnick* court reversed the district court's holding that the plaintiffs had not sufficiently pled causation and damages to survive a motion to dismiss. This holding led to a first-of-its-kind settlement of a data breach case, discussed below.[35]

While *Resnick* involved actual identity theft, the First Circuit in *Katz v. Pershing* considered a case that was filed before any data breach.[36] It held that plaintiff's allegations of an increased risk of

---

30. *Id.* at 1143.
31. Nevertheless, the district court's dismissal under *Iqbal* and *Twombly* was affirmed by the Ninth Circuit due to the plaintiffs' failure to adequately plead "actual loss or damage," a necessary element of the negligence claim, or the existence of an implied contract. Krottner v. Starbucks, 406 F. App'x 129, 131 (9th Cir. 2010).
32. Reilly v. Ceridian Corp., 2011 WL 735512 (D.N.J. Feb. 22, 2011), *aff'd*, 664 F.3d 38 (3d Cir. 2011).
33. 664 F.3d at 46.
34. Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012).
35. *See* Curry v. AvMed, Inc., 2014 U.S. Dist. LEXIS 48485 (S.D. Fla. Feb. 28, 2014) (discussed in section 17:4).
36. Katz v. Pershing, LLC, 672 F.3d 64 (1st Cir. 2012).

potential future loss due to the defendant's alleged failure to adhere to reasonable security practices and privacy regulations did not confer standing.[37] The allegations of harm were too speculative, and the plaintiff could not show impending injury.[38] According to the First Circuit, the facts alleged left too many unknown variables, including whether the plaintiff's data would actually be stolen or lost, and even then, whether the data would be misused in a way that would harm the plaintiff. The court recognized, however, that the question of standing would be more difficult if data had actually been stolen, noting the "disarray" in decisions applying an "increased risk of harm" theory to data breach cases absent identity theft.[39]

A circuit decision, of course, does not necessarily lead to uniformity in future district court decisions, and no two data breach cases are exactly alike. Sometimes seemingly subtle factors like the type of data accessed or the method of access will mean the difference between standing and no standing. For example, a network hack of a point-of-sale system containing credit and payment card information may be more likely to be exploited than a stolen laptop with encrypted, relatively more innocuous data such as work history. Accordingly, not all data breach plaintiffs in the Eleventh Circuit, for example, will be found to have standing, even after *Resnick*. Indeed, in a case arising from a hack of MAPCO Express, Inc.'s computer systems, the Northern District of Alabama found *Resnick* left it "not entirely clear . . . whether the allegation of actual identity theft alone or the allegation of actual identity theft plus the allegation of monetary damages prompted the *Resnick* majority to find that the *Resnick* plaintiffs had standing to pursue their identity theft claims."[40] The court went on to dismiss the complaint without prejudice for lack of standing, noting "this is [still] largely unchartered territory."[41]

[C] Standing Decisions in U.S. District Courts

While the Seventh and Ninth Circuits both found allegations of future risk of identity theft sufficient to confer standing, the majority of district courts have found such allegations alone are not sufficient. As the District of Louisiana observed:

> Following *Clapper*, the majority of courts faced with data breach class actions where complaints alleged personal information was accessed but where actual identity theft was not alleged . . . have

37. *Id*. at 78.
38. *Id.* at 80.
39. *Id.*
40. Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1284 (N.D. Ala. 2014).
41. *Id*.

> dismissed the complaints for lack of Article III standing [because] the mere increased risk of identity theft or identity fraud alone does not constitute a cognizable injury unless the harm alleged is certainly impending.[42]

Where allegations of potential injury are "contingent upon . . . information being obtained and then used by an unauthorized person," courts usually have not found standing.[43] In *Key v. DSW, Inc.*, for instance, the plaintiff alleged that "unauthorized persons obtained access to and acquired the information of approximately 96,000 customers."[44] She alleged she had "been subjected to a substantial increased risk of identity theft or other related financial crimes,"[45] but the court dismissed for lack of standing finding the plaintiff had not "alleged evidence that a third party intend[ed] to make unauthorized use of her financial information or of her identity."[46]

Plaintiffs also often argue that they will incur actual harm in the form of purchasing credit monitoring services. This argument is often rejected as overlooking "the fact that [the] expenditure of time and money was not the result of any present injury, but rather the anticipation of future injury that has not materialized."[47]

Even where plaintiffs allege actual fraudulent credit card charges as a result of the data breach, courts have dismissed for lack of standing where the plaintiffs were not held financially responsible for paying the fraudulent charges. In *Peters v. St. Joseph Services Corp.*, hackers infiltrated a healthcare provider's network and accessed personal information of patients and employees, including bank account information.[48] There was an attempted purchase on plaintiff's credit card, but it was declined by the plaintiff when she received a fraud alert. As such, there was no injury to confer standing, and any future

---

42. Green v. Ebay Inc., 2015 U.S. Dist. LEXIS 58047, at *1–2, *10 (E.D. La. May 4, 2015) (following "the majority of district courts" in holding "the increased risk of future identity theft or identity fraud posed by a data security breach" does not confer Article III standing) (citations omitted).
43. Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006).
44. *Id.* at 686.
45. *Id.*
46. *Id.* at 690.
47. Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1021 (D. Minn. 2006); *see also* Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8 (D.D.C. 2007). *But see Neiman Marcus*, 794 F.3d at 694 (noting "[m]itigation expenses do not qualify as actual injuries where the harm is not imminent," while finding it "telling . . . that Neiman Marcus offered one year of credit monitoring and identity-theft protection to all customers for whom it had contact information," and that that cost "easily qualifies as a concrete injury").
48. Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847 (S.D. Tex. 2015).

risk was too speculative and attenuated. Each of plaintiff's alleged harms, the court pointed out, began with the word "if."[49]

Similarly, in *Amburgy v. Express Scripts, Inc.*, the Eastern District of Missouri found that the string of "if's" linking the data breach to the alleged injuries was fatal to standing.[50] The plaintiffs in *Amburgy* filed suit after unauthorized persons accessed the defendant's database that held personal information including contact information and Social Security numbers. It was unclear what data, if any, the hackers obtained. The alleged harm—identity theft—could only come about "'if' this personal information was compromised, and 'if' such information was obtained by an unauthorized third party, and 'if' his identity was stolen as a result, and 'if' the use of his stolen identity caused him harm."[51] Finding this risk of future harm too attenuated from the data breach to confer standing, the court dismissed the case.

Still, standing decisions are mixed, even within a district. The Southern District of New York, for example, has come out on both sides. In *Hammond v. Bank of New York Mellon Corp.*, the court granted summary judgment for the defendant, dismissing all claims, and finding no Article III standing where the plaintiffs alleged only an increased risk of identity theft resulting from a loss of data.[52] *Hammond* arose out of the loss of computer back-up tapes containing personal information. A few of the named plaintiffs in *Hammond* experienced unauthorized payment card transactions, but they admitted they could not connect the unauthorized transactions to the data loss other than by a coincidence of timing. Thus, the alleged injuries stemming from the data loss remained "speculative" and "hypothetical," and the action was dismissed for lack of standing.[53] By contrast, the court two years earlier had held in *Caudle v. Towers, Perrin, Forster & Crosby, Inc.* that increased risk of future harm was sufficient to confer standing, analogizing to toxic tort cases.[54]

Distinguishing factors among the cases are not always clear, and range from legal interpretation of standing doctrine to the type of information stolen or hacked. At least one court, for instance, has interpreted the Supreme Court's *Driehaus* decision as relegating *Clapper*'s more rigorous "certainly impending" standard to national

---

49. *Id*. at 854.
50. Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046 (E.D. Mo. 2009).
51. *Id.* at 1053.
52. Hammond v. Bank of N.Y. Mellon Corp., 2010 WL 2643307, at *6–9 (S.D.N.Y. June 25, 2010).
53. *Id.* at *8.
54. Caudle v. Towers, Perrin, Forster & Crosby, Inc., 580 F. Supp. 2d 273, 281 (S.D.N.Y. 2008).

security cases.[55] The court in *Green v. eBay* distinguished decisions finding standing as involving stolen credit or debit card numbers, while the plaintiff in *Green* did not allege that any financial information was stolen.[56]

§ 17:3.2 Failure to State a Claim upon Which Relief Can Be Granted (Rule 12(b)(6))

Even where a court finds standing, however, most data breach cases are dismissed under Rule 12(b)(6) of the Federal Rules of Civil Procedure for failure to state a claim. Plaintiffs, even with standing, must still adequately plead damages and causation, necessary elements in most common law causes of action arising from data breaches. As courts have recognized, these are often difficult elements to plead, because even in cases of actual identity theft, there is little information to causally connect the data breach to the specific instance of identity theft.[57]

The Seventh Circuit in *Pisciotta*, for example, found standing with little discussion and focused instead on the question of whether the plaintiffs' alleged injuries were compensable under Indiana law. The court answered no and affirmed dismissal of the case.[58] Similarly, the Ninth Circuit allowed *Krottner v. Starbucks* to proceed after finding standing, but later affirmed dismissal for failure to adequately plead damages.[59] The *Krottner* plaintiffs failed to establish a cognizable injury for their negligence claim because the alleged injuries stemmed from the threat of future harm. The applicable state law was clear that "the mere danger of future harm, unaccompanied by present damages, will not support a negligence action."[60]

---

55. *See* Moyer v. Michaels Stores, Inc., 2014 WL 3511500, at *5 (E.D. La. July 14, 2014) (concluding that the Supreme Court's decision in *Driehaus* indicates *Clapper*'s imminence standard is a rigorous standing analysis to be applied only in cases that involve national security or constitutional issues); *see also supra* section 17:3.1[A] (discussing *Clapper* and *Driehaus*).
56. Green v. eBay, 2015 WL 2066531, n.34 (E.D. La. May 4, 2015) (distinguishing *In re* Adobe Sys., Inc. Privacy Litig., 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014), and *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014)).
57. *See Burton*, 47 F. Supp. 3d at 1280 ("Under the pleading standard that the United States Supreme Court enunciated in *Ashcroft v. Iqbal*, [556 U.S. 662 (2009),] it is difficult for consumers like Mr. Burton to assert a viable cause of action stemming from a data breach because in the early stages of an action, it is challenging for a consumer to plead facts that connect the dots between the data breach and an actual injury so as to establish Article III standing.").
58. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).
59. *Krottner*, 406 F. App'x at 131.
60. *Id*.

One of the largest data breach cases emerged a much smaller case after defendants' motion to dismiss.[61] The plaintiffs had brought fifty-one causes of action, including claims sounding in negligence, breach of contract, violation of consumer protection statutes, violation of the California Database Breach Act, and violation of the Fair Credit Reporting Act. The defendants first argued that *Clapper* tightened the standing analysis, which had been governed by the Ninth Circuit's pre-*Clapper* decision in *Krottner v. Starbucks*.[62] But the district court disagreed, finding the *Krottner* analysis in line with *Clapper*. It held that, by alleging personal information was collected and then wrongfully disclosed as a result of the data breach, plaintiffs had standing.[63]

Despite finding standing, most but not all of plaintiffs' claims were dismissed for failure to state a claim. For example, negligence theories were dismissed for failure to plead harm and causation with sufficient particularity, and under the economic loss doctrine. Still, the court upheld consumer fraud claims based on misrepresentations and omissions regarding reasonable network security and industry-standard encryption, as well as claims under the California Database Breach Act, which sets forth standards and requirements for disclosing a data breach and includes a private right of action.

In *McLoughlin v. People's United Bank, Inc.*, the applicable state law required an "ascertainable loss," and the court found an increased risk of identity theft did not constitute an ascertainable loss absent actual misuse of the stolen data.[64] The court, citing New York law, noted that "an increased risk of future identity theft is not, in itself, an injury that the law is prepared to remedy."[65] And in *Grigsby v. Valve Corp.*, the Western District of Washington dismissed a putative class action brought after a hacking incident in which a third party breached the defendant's Internet security system and accessed users' personal account information.[66] The court found that "when personal information is compromised due to a security breach, there is no cognizable harm absent actual fraud or identity theft."[67]

The *Grigsby* court addressed the plaintiffs' allegations of present harm under the *Iqbal/Twombly* pleading standards, finding insufficient general allegations of interruption to various services and

---

61. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. 2014).
62. Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010).
63. *Sony*, 996 F. Supp. 2d at 961–62.
64. McLoughlin v. People's United Bank, Inc., 2009 U.S. Dist. LEXIS 78065, at *19–20 (D. Conn. 2009).
65. *Id.* at *22.
66. Grigsby v. Valve Corp., 2012 U.S. Dist. LEXIS 179096, at *3 (W.D. Wash. 2012).
67. *Id.* at *6.

subscriptions, "loss of data, . . . an inability to access various gaming networks," and a loss of "the monies paid to Defendant for products and services which do not conform to the express warranties made by Defendant."[68] Without specific allegations regarding which services were interrupted, which networks were inaccessible, what data was lost, and how any money was lost, the complaint constituted "naked assertions" that did not give the defendant fair notice of the basis for the claims. It "did not raise entitlement to relief above the speculative level."[69]

In short, for the few cases that survive a Rule 12(b)(1) motion contesting standing, even fewer survive a 12(b)(6) motion.

§ 17:3.3 Surviving Other Motions

For the small number of cases that survive a motion to dismiss for lack of standing and failure to state a claim, procedurally the next important decision points include motions for summary judgment and for class certification. And while settlement may occur before or after the motions to dismiss are decided, for defendants that continue to defend themselves, a loss on summary judgment or on class certification generally leads to settlement.

[A] Motions for Summary Judgment

Take, for example, the case of *Forbes v. Wells Fargo Bank, N.A.*[70] The dispute in *Forbes* arose from the allegedly negligent protection of personal data. Defendant Wells Fargo Bank and subsidiaries of Wells Fargo hired a service provider, Regulus Integrated Solutions, to print monthly statements for certain home equity mortgage and student loan customers. On October 3, 2004, computers were stolen from Regulus that contained unencrypted customer information including names, addresses, Social Security numbers, and account numbers. Plaintiffs Kristine Forbes and Morgan Koop were among the customers whose information was on one of the stolen computers. After discovery, the court rejected plaintiffs' claim that their money spent on credit-monitoring services established damages, and granted defendant's motion for summary judgment, dismissing the case.[71]

[B] Motions for Class Certification

Another hurdle for consumer class action plaintiffs is class certification. Rule 23 of the Federal Rules of Civil Procedure sets forth the necessary elements for a case to proceed as a class action. The element

---

68. *Id.* at *12.
69. *Id.* at *12–13.
70. Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018 (D. Minn. 2006).
71. *Id.* at 1021.

that is often at issue in data breach cases is the predominance requirement. To certify and maintain a class action, Rule 23 requires that "the court find[ ] that the questions of law or fact common to class members predominate over any questions affecting only individual members."[72]

With respect to the predominance requirement, the case of *In re Hannaford Brothers* is instructive. There the court distinguished between individualized damages issues that would not defeat class certification and individualized causation issues that would.[73] In *Hannaford*, a grocery store was hacked, and the credit cards of the store's customers were stolen. Following a dismissal of earlier claims for lack of standing, the plaintiffs eventually sought to certify a class of people that spent money mitigating the breach by paying fees to replace their credit cards and purchasing credit and identity theft monitoring. The court found that individual issues would predominate when it came to what caused the alleged damages. It recognized that customers may have replaced their cards or purchased insurance for reasons unrelated to the breach. The court also acknowledged that credit card fraud is pervasive and may have happened for reasons unrelated to the breach. The court denied certification because the plaintiffs had not presented an expert opinion to overcome the predominance issues related to causation and damages.

The *Hannaford* court's analysis may impact settlement values because plaintiffs may need to present expert testimony to support their novel causation and damages theories before a class can be certified.

§ 17:4 Noteworthy Settlements

In the past few years, there have been numerous settlements of data breach class actions, arising at different points in the proceedings. The following is a survey of some of those settlements.

Heartland. In *In re Heartland Payment System, Inc. Customer Data Security Breach Litigation*,[74] hackers stole payment card information for 100 million consumers from a payment processing company. The Judicial Panel on Multidistrict Litigation (JPML) transferred the resulting class action lawsuits to the Southern District of Texas for consolidated pretrial proceedings. Heartland settled the case and agreed to make up to $2.4 million available to customers.

---

72. FED. R. CIV. P. 23(b)(3).
73. *In re* Hannaford Bros. Co. Customer Data Sec. Breach Litig., 293 F.R.D. 21, 26 (D. Me. 2013).
74. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 851 F. Supp. 2d 1040 (S.D. Tex. 2012).

AvMed. The 2014 settlement in *Curry v. AvMed, Inc.*[75] was considered cutting-edge because it was the first time that plaintiffs who did not suffer identify theft were allowed to claim funds. The case stemmed from a 2009 theft from health insurer AvMed of laptop computers that contained the personal information of 1.2 million customers. And while the district court had dismissed the claims in July 2011 based on a lack of injury, the Eleventh Circuit reversed and reinstated the case on the basis that the plaintiffs had made an explicit connection between the stolen materials and the subsequent opening of fake bank accounts.[76] The case subsequently settled for $3 million and included payment to customers of $10 for each year of insurance they purchased (up to a cap of $30).

Adobe. In 2013, hackers attacked Adobe's servers and spent several months inside the network without being detected, removing customer data (including payment card information) and Adobe source code in the process. Plaintiffs sued, arguing that Adobe failed to implement reasonable, industry-standard security procedures (such as employing intrusion detection systems and properly segmenting source code and customer payment card data) that would have prevented or minimized the impact of the data breach.[77] The breach affected 38 million Adobe users. The case settled after the court granted in part and denied in part Adobe's motion to dismiss.[78] The plaintiffs filed a partially redacted motion in the U.S. District Court for the Northern District of California seeking voluntary dismissal of the class claims pursuant to the no-fault settlement. Adobe agreed to pay $5,000 per named plaintiff and $1.2 million in legal fees and expenses, and agreed to additional security enhancements. The settlement is noteworthy because there was no evidence of actual damages or identity theft.

LinkedIn. In June 2012, LinkedIn announced that hackers had stolen about 6.5 million users' passwords and published them on a Russian website. Multiple class actions were consolidated in the Northern District of California. Initially, the case was dismissed because of the failure to allege cognizable harm. Subsequently, the plaintiffs filed an amended complaint claiming that LinkedIn had misled its customers about its data protection policies. After the court partially granted and partially denied LinkedIn's motion to dismiss the second amended complaint,[79] the case settled for $1.25 million. The

---

75. Curry v. AvMed, Inc., 2014 U.S. Dist. LEXIS 48485 (S.D. Fla. Feb. 28, 2014).
76. Resnick v. Avmed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012).
77. Consolidated Class Action Complaint, *In re* Adobe Sys., Inc. Privacy Litig., 2014 WL 1841156 (N.D. Cal. Apr. 4, 2014).
78. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014).
79. *In re* LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089, 1095 (N.D. Cal. 2013).

approximately 800,000 class members were able to receive up to $50 each.

Target. In December 2013, Target announced that third-party intruders had stolen credit card, debit card, and/or contact information for 110 million of its customers. Class representatives filed multiple actions alleging common law claims and violations of state laws based on Target's allegedly inadequate data security and alleged delay in notifying Target customers of the breach. The cases were consolidated in the District of Minnesota, and a settlement was achieved in 2015 after the district court's decision, which granted in part and denied in part Target's motion to dismiss.[80] Target agreed to pay $10 million to settle the claims of class members, and the maximum recovery per customer was capped at $10,000.[81] Target also agreed to pay attorney fees and expenses of up to $6.75 million.[82]

---

80. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).

81. The court granted final approval of the settlement on November 15, 2015, but an appeal of that order was filed by objectors. On January 27, 2016, the Eighth Circuit dismissed the objection, and the settlement is now final.

82. Relatedly, Target recently settled for $39.4 million the class action lawsuits brought against it by financial institutions in the payment card industry for costs they incurred to replace credit cards of affected Target customers, as well as the costs of the fraudulent charges. That settlement came about after the court denied Target's motion to dismiss, finding the financial institutions had adequately pleaded "a special relationship" with Target. Order, *In re* Target (Fin. Insts. Case), MDL 14-2522 (J.P.M.L. Dec. 2, 2014). Earlier in 2015, Target agreed to pay Visa card issuers as much as $67 million over the breach.