



Proskauer» Hedge Funds

Hedge Funds
Luncheon Series:
**Winter Regulatory
Update 2020**

Table of Contents

Winter Regulatory Update 2020

Program Materials

2020 OCIE Exam Priorities	Page 3
Recent OCIE Risk Alerts	Page 31
Form CRS	Page 57
Questions Asked in Recent SEC Exams.....	Page 76
Alternative Data	Page 79
Big Data Interview Questions.....	Page 146
California Consumer Privacy Act.....	Page 147



U.S. SECURITIES AND
EXCHANGE COMMISSION

2020 **EXAMINATION PRIORITIES**

Office of Compliance Inspections and Examinations

CONTENTS

Message From OCIE's Leadership Team	1
Importance of Compliance	1
FY 2019 Results	1
Registered Investment Adviser Coverage	3
Anticipated Impact of Significant Rulemaking	4
Risk, Technology, and Industry Trends	5
Firm and Investor Outreach and Risk Alerts	6
Introduction	8
Retail Investors, Including Seniors and Individuals Saving for Retirement	9
Fraud, Sales Practices, and Conflicts	9
Retail-Targeted Investments	10
Standards of Care	12
Information Security	13
Financial Technology (FINTECH) and Innovation, Including Digital Assets and Electronic Investment Advice	14
Digital Assets	14
Electronic Investment Advice	14
Additional Focus Areas Involving RIAs and Investment Companies	15
RIA Compliance Programs	15
Never-Before and Not Recently-Examined RIAs	15
Mutual Funds and ETFs	16
RIAs to Private Funds	16
Additional Focus Areas Involving Broker-Dealers and Municipal Advisors	16
Broker-Dealer Financial Responsibility	16
Trading and Broker-Dealer Risk Management	16
Municipal Advisors	17
AML Programs	17
Market Infrastructure	18
Clearing Agencies	18
National Securities Exchanges	19
Regulation Systems Compliance and Integrity (SCI)	19
Transfer Agents	20
Focus on FINRA and MSRB	21
FINRA	21
MSRB	21
Conclusion	22

DISCLAIMER: This statement represents the views of the staff of the Office of Compliance Inspections and Examinations. It is not a rule, regulation, or statement of the U.S. Securities and Exchange Commission (Commission). The Commission has neither approved nor disapproved its content. This statement, like all staff guidance, has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person.



MESSAGE FROM OCIE'S LEADERSHIP TEAM

The Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (SEC) is pleased to announce our examination priorities for fiscal year (FY) 2020, marking the 8th year of their publication. We hope you find our discussion of key risks, trends, and examination priorities valuable in overall efforts to promote and improve compliance and ultimately protect investors.

Importance of Compliance

As a threshold matter, we would like to emphasize that compliance programs, chief compliance officers, and other compliance staff play critically important roles at firms. Indeed, culture and tone from the top are key. In the course of conducting thousands of examinations of many different types of firms, the hallmarks of effective compliance become apparent. One such hallmark includes compliance's active engagement in most facets of firm operations and early involvement in important business developments, such as product innovation and new services. Another is a knowledgeable and empowered chief compliance officer with full responsibility, authority, and resources to develop and enforce policies and procedures of the firm. And perhaps most importantly, a commitment to compliance from C-level and similar executives to set a tone from the top that compliance is integral to the organization's success and that there is tangible support for compliance at all levels of an organization.

DID YOU KNOW?

A hallmark of effective compliance is a commitment from senior executives to set the tone that compliance is integral to the organization's success.

FY 2019 Results

For OCIE, quality is the most important aspect of the work we perform. Examiners ask themselves: Did our risk scoping correctly capture the highest risks at a firm? Did we appropriately expand our scope as we identified significant risks not initially scoped? Did we spend sufficient time and devote appropriate staffing resources (both in technical experience and team size) to ensure an effective examination? Did we promote compliance? And ultimately, did we identify errors, fraud or misappropriation at the firm, if present? Examiners ask these and countless other questions before closing an examination, all with the primary purpose of achieving OCIE's investor protection mission.

OCIE is mindful that numbers never tell the complete story of our effectiveness and efficiency. While certain statistics are discussed below, they do not completely capture or measure the quality of our examination program. Statistics do, however, convey certain reference points that provide some insights into our examination program. OCIE completed 3,089 examinations in FY 2019, which is a 2.7 percent decrease from FY 2018. This relatively minor decrease, when viewed in light of an approximate month-long suspension of virtually all examination activity due to a lapse in appropriations, is illustrative of the OCIE staff's hard work, continued improved efficiency, resiliency and dedication to the SEC's and OCIE's mission to protect investors. Examinations of registered investment advisers (RIAs) in FY 2019 remained strong at approximately 2,180, covering 15 percent of this population. Examinations of investment companies increased this year to over 150, increasing by approximately 12 percent, driven primarily by the six initiatives OCIE announced in November 2018.¹ OCIE completed over 350 examinations of broker-dealers, 110 examinations of national securities exchanges, and over 90 examinations of municipal advisors and transfer agents. OCIE also completed over 160 examinations of the Financial Industry Regulatory Authority (FINRA), including examinations of critical FINRA program areas as well as oversight reviews of FINRA examinations. Finally, OCIE completed 15 examinations of clearing agencies.

DID YOU KNOW?

The quality of examinations is the most important aspect of OCIE's work.

Through its examinations, OCIE is promoting compliance and making a difference for investors and our securities markets. For example, during FY 2019, OCIE issued more than 2,000 deficiency letters, with many firms taking direct corrective actions in response to those letters, including

by amending compliance policies and procedures or a regulatory filing; enhancing their disclosures; or, returning fees back to investors, among other things. To fight against fraud and misappropriation of investor assets, OCIE also commits significant resources to verify the existence of investor assets at custodians and to ensure that they are valued properly, a process called asset verification. In FY 2019, OCIE verified over 3.1 million investor accounts, totaling over \$1.5 trillion. Similarly, when RIAs have access to client funds or securities, OCIE prioritizes examination for compliance with the Custody Rule (Rule 206(4)-2 under the Investment Advisers Act of 1940 (Advisers Act)), which includes important client safeguards like third party audits and surprise examinations. For broker-dealers, OCIE reviews for compliance with the Customer Protection Rule (Rule 15c3-3 under the Securities Exchange Act of 1934 (Exchange Act)) and the Net Capital Rule (Rule 15c3-1 under the Exchange Act) to help ensure that customer securities and assets exist and are protected from misappropriation and that firms are adequately capitalized.

¹ <https://www.sec.gov/ocie/announcement/ocie-risk-alert-registered-investment-company-initiative>

Another way OCIE promotes compliance and protects investors is by encouraging firms to make investors whole when fees have been improperly calculated and charged. Examinations closed in FY 2019 have so far resulted in firms returning more than \$70 million to investors. When its findings are significant with respect to such improper charges or other issues, however, OCIE may refer these matters to the Division of Enforcement.

Many important Enforcement matters have resulted from OCIE examinations and referrals, including, for example: the SEC's first two settled Enforcement actions with clearing agencies; two settled matters involving Regulation SCI; dozens of settled matters involving RIAs' selection of higher cost mutual fund share classes for clients when lower cost options were available; the first settled actions brought against providers of electronic investment advice; dozens of settled actions against advisers to private funds; and settled actions against broker-dealers that misappropriated retail client funds. More than 150 enforcement referrals from FY 2019 examinations have been made so far, and we anticipate more to come. Recoveries and referral metrics may lag fiscal year reporting as OCIE continues to work to get results for harmed investors, which, for example, included 30 additional referrals and \$13 million in recoveries in FY 2019 from examinations that were completed in FY 2018.

Registered Investment Adviser Coverage

OCIE reports annually the percentage of the population of RIAs examined each year. This metric is important as OCIE is the primary, and often only, regulator responsible for supervising this segment of financial firms. The population of RIAs has grown significantly in recent years, as has the amount of assets those RIAs manage. More specifically, in just the last five years, the number of RIAs OCIE oversees increased from about 11,500 to 13,475, and the assets under management of RIAs increased from approximately \$62 trillion to \$84 trillion.

DID YOU KNOW?

In FY 2019, OCIE completed over 3,000 examinations.

In addition to this significant growth, the financial industry and marketplace are constantly evolving and responding to investor needs, regulatory changes, technology, and competition. RIAs' complexity, interconnectivity, and dependency on a variety of market participants also continue to grow: more than 3,700 RIAs manage over \$1 billion in assets; approximately 36 percent of RIAs manage a private fund; more than 55 percent of RIAs have custody of client assets; more than 60 percent of RIAs are affiliated with other financial industry firms; and approximately 12 percent of RIAs provide advisory services to a mutual fund, exchange-traded fund, or other registered investment company.

Despite this significant growth and complexity, OCIE has made significant strides over the past several years to increase its RIA coverage, including through: (1) implementation of program efficiencies, both through process and technology; (2) realignment of internal staffing to address the coverage rates for RIAs; and (3) continued investment in our human capital, through ongoing training of staff and the onboarding of experienced subject matter experts, among other things. These efforts are paying dividends: OCIE has increased its examination coverage of RIAs over the past several years from 10 percent in FY 2014 to a high of 17 percent in FY 2018. OCIE's coverage of RIAs in FY 2019, a year in which the RIA population continued to increase and the SEC experienced a 35-day lapse in appropriations, was 15 percent.

While OCIE will continue to make improvements in efficiency, there remains a significant risk that, in light of industry growth and increased complexity and other factors, it does not have sufficient resources to adequately cover the RIA space. OCIE's coverage rates will likely not keep pace with the continued growth in the population and complexity, without corresponding staffing increases. While OCIE has made great strides to improve the coverage rate, the risks of diminished coverage, quality, and effectiveness are possible without further support. Ultimately, this trend is concerning and a focus for OCIE and Chairman Clayton.

Anticipated Impact of Significant Rulemaking

The Commission finalized many new rules and interpretations in FY 2019 that will impact firms and OCIE. The most significant is the package of rulemakings and interpretations designed to enhance the quality and transparency of retail investors' relationships with RIAs and broker-dealers, bringing the legal requirements and mandated disclosures in line with reasonable investor expectations, while preserving access, in terms of choice and cost, to a variety of investment services and products. Specifically, these actions include new Regulation Best Interest, the new Form CRS Relationship Summary, and two separate interpretations under the Advisers Act, which will be FY 2020 examination priorities.

OCIE recognizes that these new rules will require various market participants to make changes to their operations, including to required disclosures, marketing materials and compliance programs. In order to assist firms with planning for compliance with these new rules, the SEC established an inter-Divisional Standards of Conduct Implementation Committee—of which staff across OCIE are members. We encourage firms to actively engage with OCIE and other SEC staff as they plan for implementation. Questions may be submitted by email to: IABDQuestions@sec.gov.

Risk, Technology, and Industry Trends

In FY 2020, OCIE will continue to monitor industry developments and market events to assess impact on retail investors and SEC-registered firms, and continue to tailor its risk-based program to respond. The footprint of registered entities has become more global and diverse, often with an increased dependency on services and operations worldwide. And the use of third-party service providers and other vendors by registrants continues to increase, which can bring improved expertise and effectiveness, but also additional challenges and risks to organizations. OCIE will continue to focus on third-party risk management in FY 2020. OCIE will also closely track and evaluate the impact of several major risk themes affecting its registrant population, including information security and resiliency risks, geopolitical events, and the industry's transition away from LIBOR. OCIE, in coordination with other SEC Divisions and Offices, will engage with firms on these risks, among others, to better assess impact and what, if any, compliance challenges develop.

OCIE continues to make investments in human capital, technology and data analytics. In FY 2019, OCIE added over twenty-seven new staff positions, and it anticipates that these hires will each bring a wealth and variety of experience and knowledge to the examination program. OCIE's technology tools and data analytics work also continue to mature and help drive many of its risk identification efforts, initiatives and examination processes. All of these resources help OCIE identify potential stresses on compliance programs and operations, conflicts of interest, and conduct issues that may ultimately harm investors.

As OCIE continues to advance its use of technology and data analytics, it is mindful of its responsibility to ensure that information requested during an examination is appropriately calibrated and, once information is provided, is protected. During an examination, staff may request certain books and records that include sensitive information such as customer transactions, communications and other personal data to assess whether firms are complying with the federal securities laws. OCIE strives to appropriately tailor its requests for data and encourages dialogue with staff where a registrant may have a preferred or alternative data solution that would meet examination objectives.

While balancing the importance of data protection with effectively protecting investors, OCIE has experienced challenges with examining non-U.S. registrants that are increasingly subject to laws on data protection and privacy, among others, that may impact the cross-border transfers of certain information. These challenges are particularly acute with the growing population of off-shore RIAs that now number close to 1,000, managing

over \$10 trillion in investor assets. U.S. securities laws, SEC rules, and registration forms require non-U.S. RIAs to certify that they will provide to the SEC required records necessary for inspection. In light of this conflict of law, OCIE is seeking additional information from non-U.S. applicants for RIA registration to ensure these firms can comply with inspection requirements of U.S. securities laws, which are designed to protect impacted investors. The SEC continues to work with both industry and its counterparts in other countries to address this challenge.

Firm and Investor Outreach and Risk Alerts

OCIE's priorities provide an overview of key areas where it intends to focus its limited resources. That said, the stated priorities and other examinations OCIE conducts do not encompass all of OCIE's efforts to improve compliance. To promote compliance, and to further the effective and efficient allocation of examination resources, OCIE proactively engages with registrants through outreach events, including national and regional compliance seminars. In FY 2019, OCIE staff participated in or held more than 100 such outreach events. OCIE staff also conducted outreach to investors, including specific efforts directed toward members of the military and teachers, designed to inform them about retirement planning and investment basics.

OCIE also engaged with and informed the industry through risk alerts in efforts to raise awareness of compliance and industry risks. During FY 2019, OCIE published the following eight risk alerts, which represent the most risk alerts in a year since it began publishing them in FY 2011.

- Investment Adviser Compliance Issues Related to the Cash Solicitation Rule;
- Risk-Based Examination Initiatives Focused on Registered Investment Companies;
- Observations from Investment Adviser Examinations Relating to Electronic Messaging;
- Transfer Agent Safeguarding of Funds and Securities;
- Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P—Privacy Notices and Safeguard Policies;
- Safeguarding Customer Records and Information in Network Storage—Use of Third Party Security Features;
- Observations from Examinations of Investment Advisers: Compliance, Supervision, and Disclosure of Conflicts of Interest; and
- Investment Adviser Principal and Agency Cross Trading Compliance Issues.

OCIE will continue its publication of risk alerts that both describe its national initiatives as well as outline findings from examinations in key areas with the hopes that sharing this information will further promote compliance within registered firms and ultimately further protect the investing public.

Finally, please know that OCIE is always interested in hearing more about new and emerging risk areas and products as well as how it can be more effective in its mission. OCIE's contact information can be found at: <https://www.sec.gov/contact-information/sec-directory>. Please engage with our staff. If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify SEC staff at <https://www.sec.gov/tcr>. And thank you for doing your part to protect investors and promote compliance.



INTRODUCTION

In 2020, OCIE will prioritize the examination of certain practices, products, and services that it believes present potentially heightened risks to investors or the integrity of the U.S. capital markets. Examinations of these priority areas are designed to support the SEC’s mission to protect investors, facilitate capital formation, and maintain fair, orderly, and efficient markets.

Many of the themes noted below are perennial risk areas OCIE routinely covers in its examinations. Their importance to retail investors, the seriousness and frequency of prior years’ examination findings, or both, demonstrate the need for OCIE to continue to be vigilant in these significant areas. Moreover, the priorities described below are not exhaustive and will not be the only issues OCIE addresses in its examinations, published risk alerts, and investor and industry outreach.

DID YOU KNOW?

In FY 2019, OCIE achieved examination coverage of approximately 15 percent of registered investment advisers.

While the priorities drive many of OCIE’s examinations, the selection of firms to examine and the related scoped risk areas of focus are determined through OCIE’s risk-based analysis. OCIE’s risk-based approach varies depending on the type of registered firm and the nature of its business.

For RIAs and broker-dealers, OCIE considers dozens of potential risk factors, which can include: products and services offered, including certain products identified as higher risk; compensation and funding arrangements; prior examination observations and conduct; disciplinary history of associated individuals and affiliates of a registered firm; changes in firm leadership or other personnel; and, whether a firm has access to investor assets, *i.e.*, custody. While the aforementioned characteristics and factors are not exhaustive, they provide insight into criteria that OCIE considers in its risk assessment process. OCIE’s risk-based approach results in examinations that are focused on key aspects of the SEC’s regulatory oversight, such as the adequacy of disclosures concerning services, fees and expenses; firms’ management and handling of conflicts of interest for RIAs; and sales practice, trading and execution quality issues for broker-dealers.

OCIE’s analytic efforts and examinations remain firmly grounded in its four pillars: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy. The risk-based approach, both in selecting registrants as examination candidates and in scoping risk areas to examine, provides OCIE with greater flexibility to cover emerging and exigent risks to investors and the marketplace as they arise. For example, as our registrants and other market participants transition away from LIBOR as a widely

used reference rate in a number of financial instruments to an alternative reference rate, OCIE will be reviewing firms' preparations and disclosures regarding their readiness, particularly in relation to the transition's effects on investors. Some registrants have already begun this effort and OCIE encourages each registrant to evaluate its organization's and clients' exposure to LIBOR, not just in the context of fallback language in contracts, but its use in benchmarks and indices; accounting systems; risk models; and client reporting, among other areas. Insufficient preparation could cause harm to retail investors and significant legal and compliance, economic and operational risks for registrants.

RETAIL INVESTORS, INCLUDING SENIORS AND INDIVIDUALS SAVING FOR RETIREMENT

OCIE will again emphasize the protection of retail investors, particularly seniors and those saving for retirement. Concentrated in our two largest program areas, the Investment Adviser-Investment Company (IAIC) and Broker-Dealer and Exchange programs, OCIE will prioritize examinations:

- Of intermediaries that serve retail investors, namely RIAs, broker-dealers, and dually-registered firms, and
- Focused on investments marketed to, or designed for retail investors, such as mutual funds and exchange-traded funds (ETF), municipal securities and other fixed income securities, and microcap securities.

Fraud, Sales Practices, and Conflicts

It is critically important that registered firms provide investors with the disclosures required by the federal securities laws, including those relating to fees and expenses, and conflicts of interest, which will help enable the investing public to make better informed choices. Registered firms must effectively implement controls and systems to ensure those disclosures are made as required and that a firm's actions match those disclosures.

Examinations will focus on recommendations and advice given to retail investors, with a particular focus on: (1) seniors, including recommendations and advice made by entities and individuals targeting retirement communities; and (2) teachers and military personnel. Additionally, OCIE will focus on higher risk products—including private placements and

DID YOU KNOW?

In FY 2019, OCIE verified over 3.1 million investor accounts, totaling over \$1.5 trillion.

securities of issuers in new and emerging risk areas—such as those that: (1) are complex or non-transparent; (2) have high fees and expenses; or (3) where an issuer is affiliated with or related to the registered firm making the recommendation. Examinations will relatedly focus on registered firms’ disclosures and supervision of outside business activities of its employees and associated persons, and any conflicts that may arise from those activities.

OCIE will also continue to examine RIAs to assess whether, as fiduciaries, they have fulfilled their duties of care and loyalty. This will include assessing, among other things, whether RIAs provide advice in the best interests of their clients and eliminate, or at least expose through full and fair disclosure, all conflicts of interest which might incline an RIA, consciously or unconsciously, to render advice which is not disinterested. That RIAs are acting in a manner consistent with their fiduciary duty and meeting their contractual obligations to their clients is paramount to maintaining investor confidence in the markets and investment professionals. OCIE, therefore, will continue to focus on risks associated with fees and expenses, and undisclosed, or inadequately disclosed, compensation arrangements.

DID YOU KNOW?

In FY 2019, OCIE completed over 150 examinations of investment companies (IC) and conducted six national IC initiatives.

Fee and compensation-based conflicts of interest may take many forms, including revenue sharing arrangements between a registered firm and issuers, service providers, and others, and direct or indirect compensation to advisory personnel for executing client transactions. In addition, duty of care concerns may arise when an RIA does not aggregate certain accounts for purposes of calculating fee discounts in accordance with its disclosures. These potential breaches of fiduciary duty may adversely impact portfolio management costs, reduce investor returns, and inappropriately influence investment decision-making.

Retail-Targeted Investments

Certain securities products can pose elevated risks when marketed or sold to retail investors, whether as a result of the characteristics of those securities, the dynamics in the markets, or due to the significant amount or concentration of assets retail investors have invested in a product. As in past years, OCIE will continue to prioritize examinations

of issues focused on retail investors, including those related to mutual funds and ETFs, municipal securities and other fixed income securities, and microcap securities.

Mutual Funds and ETFs

Mutual funds and ETFs are the primary investment vehicle for many retail investors. In addition to the other mutual fund and ETF priorities identified below, OCIE will continue to prioritize the examination of financial incentives provided to financial services firms and professionals that may influence the selection of particular mutual fund share classes. OCIE also will review for mutual fund fee discounts that should be provided to investors as a result of policies, contractual or disclosed breakpoints, such as discounts provided based on achieving managed investments of a specific size.

Municipal Securities and Other Fixed Income Securities

OCIE will examine broker-dealer trading activity in municipal and corporate bonds for compliance with best execution obligations; fairness of pricing, mark-ups and mark-downs, and commissions; and confirmation disclosure requirements, including retail disclosures relating to mark-ups and mark-downs.

Microcap Securities

OCIE will examine broker-dealers and transfer agents to review for those that may be engaged in, or aiding and abetting, pump and dump schemes, market manipulation, and illegal distributions of securities of smaller market capitalization companies—*i.e.*, companies with a market capitalization under \$250 million. Broker-dealers may be selected for examination based on factors such as employing registered representatives with disciplinary history, engaging in significant trading activity in unlisted securities, and making markets in unlisted securities. Focus areas for examinations will include: transfer agent handling of microcap distributions and share transfers; broker-dealer sales practices; broker-dealer supervision of high risk registered representatives; and broker-dealer compliance with certain regulatory requirements, including those concerning quotations under Rule 15c2-11 Exchange Act, the locate requirement of Regulation SHO, and the obligation to file suspicious activity reports (SARs).

Standards of Care

The Commission's June 2019 adoption of Regulation Best Interest, the Interpretation Regarding Standard of Conduct for Investment Advisers, and the Form CRS Relationship Summary will have a direct impact on the retail investor experience with broker-dealers and RIAs.² Regulation Best Interest requires broker-dealers, or a natural person who is an associated person of a broker or dealer, among other things, to act in the best interest of their retail customers when making a recommendation of any securities transaction or investment strategy involving securities without placing their financial or other interests ahead of the interests of the retail customer. The standard of conduct draws from key fiduciary principles and cannot be satisfied through disclosure alone. The Interpretation Regarding Standard of Conduct for Investment Advisers reaffirms, and in some cases clarifies, aspects of an RIA's fiduciary duty that comprises duties of care and loyalty to their clients.

In order to assist firms with planning for compliance with the new rules, the SEC established an inter-Divisional Standards of Conduct Implementation Committee, of which OCIE representatives are members.³ To further assist broker-dealers before the June 30, 2020 compliance date for Regulation Best Interest and Form CRS, OCIE will engage with broker-dealers during examinations on their progress on implementing the new rules and questions they may have regarding the new rules. After the compliance dates, OCIE intends to assess implementation of the requirements of Regulation Best Interest, including policies and procedures regarding conflicts disclosures, and for both broker-dealers and RIAs, the content and delivery of Form CRS. Moreover, OCIE has already integrated the Interpretation Regarding Standard of Conduct for Investment Advisers into the IAIC examination program.

² See Regulation Best Interest: The Broker-Dealer Standard of Conduct, Rel. No. 34-86031 (June 5, 2019), available at <https://www.sec.gov/rules/final/2019/34-86031.pdf>; Commission Interpretation Regarding Standard of Conduct for Investment Advisers, Rel. No. IA-5248 (June 5, 2019), available at <https://www.sec.gov/rules/interp/2019/ia-5248.pdf>; Form CRS Relationship Summary; Amendments to Form ADV, Rel. No. 34-86032 (June 5, 2019), available at <https://www.sec.gov/rules/final/2019/34-86032.pdf>.

³ The SEC encourages firms to actively engage with this committee as questions arise in planning for implementation. You may send your questions by email to IABDQuestions@sec.gov.

INFORMATION SECURITY

Information security is critical to the operation of the financial markets and the confidence of its participants. The impact of a breach in information security, including a successful cyber-attack, may have consequences that extend beyond the firm compromised to other market participants and retail investors, who may not be well informed of these risks and the potential consequences. OCIE is focused on working with firms to identify and address information security risks, including cyber-related, and to encourage market participants to actively and effectively engage regulators and law enforcement in this effort.

DID YOU KNOW?

OCIE prioritized information security in each of its five examination programs in FY 2019.

OCIE will continue to prioritize information security in each of its five examination programs. Examinations will focus on, among other things, proper configuration of network storage devices, information security governance generally, and retail trading information security. Specific to RIAs, OCIE will continue to focus its examinations on assessing RIAs' protection of clients' personal financial information. Particular focus areas will include: (1) governance and risk management; (2) access controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response and resiliency.

In the area of third-party and vendor risk management, OCIE will also focus on oversight practices related to certain service providers and network solutions, including those leveraging cloud-based storage. OCIE will continue to conduct examinations of registrants to review for compliance with Regulations S-P and S-ID. OCIE also will focus on the controls surrounding online access and mobile application access to customer brokerage account information. Finally, OCIE will examine for the safeguards around the proper disposal of retired hardware that may contain client information and potential network information that could create an intrusion vulnerability.

FINANCIAL TECHNOLOGY (FINTECH) AND INNOVATION, INCLUDING DIGITAL ASSETS AND ELECTRONIC INVESTMENT ADVICE

Innovations and advancements in financial technologies, methods of capital formation, market structures, and investor interfaces continue to grow at a rapid pace. For example, registered firms are increasingly using new sources of data, often referred to as “alternative data” by the industry that, among other things, may drive investment decision-making. OCIE remains focused on keeping abreast of these developments, and examinations will focus on firms’ use of these data sets and technologies to interact with and provide services to investors, firms, and other service providers and assess the effectiveness of related compliance and control functions.

Digital Assets

The digital assets market has grown rapidly and presents various risks, including for retail investors who may not adequately understand the differences between these assets and more traditional products. Due to these risks, OCIE will continue to identify and examine SEC-registered market participants engaged in this space. Examinations will assess the following: (1) investment suitability, (2) portfolio management and trading practices, (3) safety of client funds and assets, (4) pricing and valuation, (5) effectiveness of compliance programs and controls, and (6) supervision of employee outside business activities.

Electronic Investment Advice

In addition, OCIE will continue its focus on RIAs that provide services to their clients through automated investment tools and platforms, often referred to as “robo-advisers.” Areas of focus include, among others: (1) SEC registration eligibility, (2) cybersecurity policies and procedures, (3) marketing practices, (4) adherence to fiduciary duty, including adequacy of disclosures, and (5) effectiveness of compliance programs.

ADDITIONAL FOCUS AREAS INVOLVING RIAs AND INVESTMENT COMPANIES

OCIE typically assesses compliance programs of RIAs in one or more core areas, including the appropriateness of account selection, portfolio management practices, custody and safekeeping of client assets, best execution, fees and expenses, and valuation of client assets for consistency and appropriateness of methodology. In addition, OCIE will often assess the adequacy of disclosures and governance practices in the core areas reviewed.

RIA Compliance Programs

OCIE will continue to review the compliance programs of RIAs, including whether those programs and their policies and procedures, are reasonably designed, implemented, and maintained.

OCIE will continue to prioritize examinations of RIAs that are dually registered as, or are affiliated with, broker-dealers, or have supervised persons who are registered representatives of unaffiliated broker-dealers. Areas of focus will include whether the firms maintain effective compliance programs to address the risks associated with best execution, prohibited transactions, fiduciary advice, or disclosure of conflicts regarding such arrangements. OCIE will also prioritize examining firms that utilize the services of third-party asset managers to advise clients' investments to assess, among other things, the extent of these RIAs' due diligence practices, policies, and procedures.

DID YOU KNOW?

OCIE staff participated in or held more than 100 compliance outreach events in FY 2019.

OCIE has a particular interest in the accuracy and adequacy of disclosures provided by RIAs offering clients new types or emerging investment strategies, such as strategies focused on sustainable and responsible investing, which incorporate environmental, social, and governance (ESG) criteria.

Never-Before and Not Recently-Examined RIAs

OCIE will continue to conduct risk-based examinations of RIAs that have never been examined, including new RIAs and RIAs registered for several years that have yet to be examined. OCIE will also prioritize examinations of RIAs that were previously examined but have not been examined for a number of years to focus on whether the RIAs' compliance programs have been appropriately adapted in light of any substantial growth or change in their business models.

Mutual Funds and ETFs

As retail assets continue to flow into investment companies, OCIE will prioritize examinations of mutual funds and ETFs, the activities of their RIAs, and oversight practices of their boards of directors. Examinations will assess industry practices and regulatory compliance in various areas, including a focus on: (1) RIAs that use third-party administrators to sponsor the mutual funds they advise or are affiliated with; (2) mutual funds or ETFs that have not previously been examined; and (3) RIAs to private funds that also manage a registered investment company with a similar investment strategy.

RIAs to Private Funds

OCIE will continue to focus on RIAs to private funds that have a greater impact on retail investors, such as firms that provide management to separately managed accounts side-by-side with private funds. Moreover, OCIE will review RIAs to private funds to assess compliance risks, including controls to prevent the misuse of material, non-public information and conflicts of interest, such as undisclosed or inadequately disclosed fees and expenses, and the use of RIA affiliates to provide services to clients.

ADDITIONAL FOCUS AREAS INVOLVING BROKER-DEALERS AND MUNICIPAL ADVISORS

In addition to the aforementioned areas focusing on sales practices, broker-dealer examinations will also focus on the safety of customer cash and securities, risk management, certain types of trading activity, the effects of evolving commissions and other cost structures, best execution, and payment for order flow arrangements.

Broker-Dealer Financial Responsibility

Broker-dealers that hold customer cash and securities have a responsibility to ensure that those assets are safeguarded in accordance with the Customer Protection Rule and the Net

Capital Rule. Examinations of broker-dealers will continue to focus on compliance with these rules, including the adequacy of internal processes, procedures, and controls.

Trading and Broker-Dealer Risk Management

OCIE will also examine firms' trading and risk management practices. For example, OCIE will examine firms' trading and other activities in "odd lots," that is, orders under 100 shares. These orders often represent retail interest and require special treatment by broker-dealers to ensure compliance with applicable

DID YOU KNOW?

OCIE will continue to publish Risk Alerts describing its national initiatives and outlining findings from examinations in key areas. We believe sharing this information further promotes compliance and protects investors.

laws and regulations, including best execution. OCIE will also continue to examine for controls around the use of automated trading algorithms by broker-dealers. Algorithmic trading has expanded into multiple asset classes and is subject to SEC and FINRA rules governing trading activity. Poorly designed trading algorithms have the potential to adversely impact market and broker-dealer stability. OCIE will, therefore, examine how broker-dealers supervise algorithmic trading activities, including the development, testing, implementation, maintenance, and modification of the computer programs that support their automated trading activities and controls around access to computer code. Finally, OCIE will examine registered firms' use of internal procedures, practices, and controls to manage trading risk.

Municipal Advisors

Municipal advisors provide advice to, or on behalf of, a municipal entity or obligated person with respect to municipal financial products or the issuance of municipal securities or municipal financial products. OCIE will continue to conduct examinations of municipal advisors, concentrating on whether they have satisfied their registration, professional qualification, and continuing education requirements. OCIE will prioritize the review of municipal advisor fiduciary duty obligations to municipal entity clients, fair dealing with market participant requirements, and the disclosure of conflicts of interest. OCIE will also focus on the conduct of municipal advisors when faced with conflicts while representing their clients, and compliance with recently-effective Municipal Securities Rulemaking Board (MSRB) Rule G-40 concerning advertisements.

AML PROGRAMS

The Bank Secrecy Act requires financial institutions, including broker-dealers and investment companies, to establish anti-money laundering (AML) programs. These programs must, among other things, include policies and procedures reasonably designed to identify and verify the identity of customers and beneficial owners of legal entity customers, perform customer due diligence (as required by the Customer Due Diligence rule), monitor for suspicious activity, and, where appropriate, file SARs with the Financial Crimes Enforcement Network. SARs are used to detect and combat terrorist financing, public corruption, market manipulation, and a variety of other fraudulent behavior.

Given the importance of these requirements, OCIE will continue to prioritize examining broker-dealers and investment companies for compliance with their AML obligations in order to assess, among other things, whether firms have established appropriate customer identification programs and whether they are satisfying their SAR filing obligations, conducting due diligence on customers, complying with beneficial ownership requirements, and conducting robust and timely independent tests of their AML programs. The goal of these

examinations is to ensure that broker-dealers and investment companies have adequate policies and procedures in place that are reasonably designed to identify suspicious activity and illegal money-laundering activities.

MARKET INFRASTRUCTURE

Clearing Agencies

Title VIII of the Dodd-Frank Act requires the SEC to examine, at least once annually, registered clearing agencies that the Financial Stability Oversight Council has designated as systemically important and for which the SEC serves as the supervisory agency (SEC SIFMU Clearing Agencies). Pursuant to Section 807 of the Dodd-Frank Act, the Commission must conduct exams of SEC SIFMU Clearing Agencies in order to assess, among other things: (1) the financial and operational risks borne and presented by them to financial institutions, critical markets and the financial system; (2) their resources and capabilities to monitor and control such risks; (3) the safety and soundness of the organization; and (4) their compliance with the Exchange Act, the rules and regulations promulgated under the Exchange Act, and the Dodd-Frank Act. OCIE fulfills the SEC's requirements under the Dodd-Frank Act through examinations conducted by its Office of Clearance and Settlement and its Technology Controls Program.

DID YOU KNOW?

OCIE encourages market participants to actively and effectively engage regulators and law enforcement in identifying and addressing information security risks.

OCIE will conduct risk-based exams focusing on SEC SIFMU Clearing Agency's core risks, processes, and controls which touch on each requirement of the Dodd-Frank Act. OCIE will also conduct risk-based examinations of other registered clearing agencies.

The Standards for Covered Clearing Agencies are codified in the Exchange Act, and require most registered clearing agencies to, among other things, maintain sufficient financial resources, protect against credit risks, manage member defaults, and manage operational and other risks. Examinations of SEC registered clearing agencies will focus on, where applicable: (1) compliance with the SEC's Standards for Covered Clearing Agencies and other federal securities laws applicable to registered clearing agencies; (2) whether clearing agencies have taken timely appropriate corrective action in response to prior examinations; and (3) other areas identified in collaboration with the SEC's

Division of Trading and Markets and with other regulators. Areas of focus will include liquidity risk management, collateral and investment risk management, default risk management, cyber security and resiliency, and recovery and wind down procedures more generally, among other things.

As part of its examinations, OCIE will also examine registered clearing agencies' governance, legal, compliance and risk management frameworks by reviewing these entities' efforts to escalate deficiencies identified by OCIE and internal auditors and whether they have taken timely and appropriate action to correct those deficiencies and mitigate the risks associated with those deficiencies.

Finally, OCIE consults with the Federal Reserve Board each year on the scope and methodology of the SEC's Dodd-Frank examinations, as required by that Act, and routinely consults with the SEC's Division of Trading and Markets concerning risks it observes in its supervisory role over the above clearing agencies. These risks are incorporated into the risk-based planning of the examinations discussed above.

National Securities Exchanges

National securities exchanges provide marketplaces for facilitating securities transactions and, under the federal securities laws, serve as self-regulatory organizations responsible for enforcing compliance by their members with the federal securities laws and rules and the exchanges' own rules. OCIE will examine the operations of national securities exchanges, especially how they react to market disruptions. OCIE will also examine how the national securities exchanges monitor member activity for compliance with the federal securities laws and rules and will focus on exchange efforts concerning abusive, manipulative, and illegal trading practices to protect the integrity of the marketplace.

Regulation Systems Compliance and Integrity (SCI)

Regulation SCI was adopted by the Commission to strengthen the technology infrastructure of the U.S. securities markets. Among other things, it requires SCI entities, which include national securities exchanges, registered and certain exempt clearing agencies, FINRA, MSRB, plan processors, and alternative trading systems that meet certain volume thresholds, to establish, maintain, and enforce written policies and procedures designed to ensure that their systems' capacity, integrity, resiliency, availability, and security is adequate to maintain their operational capability and promote the maintenance of fair and orderly

markets. When certain personnel at these entities have a reasonable basis to conclude that certain events have occurred, these entities are required to begin to take appropriate corrective action to remedy the event as soon as reasonably practicable and immediately notify the SEC of the occurrence.

OCIE will continue to evaluate whether SCI entities have established, maintained, and enforced written SCI policies and procedures as required. Areas of focus will include IT inventory management, IT governance, incident response, and third party vendor management, including the utilization of cloud services. OCIE will also continue to perform examinations to review whether SCI entities have taken appropriate action in response to past examinations.

Transfer Agents

Transfer agents serve as agents for securities issuers and play a critical role in the settlement of securities transactions. Among their key functions, transfer agents are responsible for maintaining issuers' securityholder records, recording changes of ownership, canceling and issuing certificates, distributing dividends and other payments to securityholders, and facilitating communications between issuers and securityholders.

OCIE will continue to examine transfer agents' core functions, including: the timely turnaround of items and transfers, recordkeeping and record retention, and safeguarding of funds and securities. OCIE examinations will also focus on the requirement for transfer agents to annually file a report by an independent accountant concerning the transfer agent's system of internal accounting controls, as well as compliance with obligations to search for lost securityholders and provide notice to unresponsive payees.

Examination candidates will include transfer agents that serve as paying agents for issuers, transfer agents developing blockchain technology, and transfer agents that provide services to issuers of microcap securities, private offerings, crowdfunded securities, or digital assets.

FOCUS ON FINRA AND MSRB

FINRA

FINRA oversees approximately 3,600 brokerage firms, 156,000 branch offices, and 630,000 registered representatives through examinations, enforcement, and surveillance. In addition, FINRA, among other things, provides a forum for securities arbitration and mediation, conducts market regulation, including by contract for a majority of national securities exchanges, reviews broker-dealer advertisements, administers the testing and licensing of registered persons, and operates industry utilities such as Trade Reporting Facilities.

OCIE conducts risk-based oversight examinations of FINRA. It selects areas within FINRA to examine through a risk assessment process designed to identify those aspects of FINRA's operations important to the protection of investors and market integrity. The analysis is informed by collecting and analyzing extensive information and data, regular meetings with key functional areas within FINRA, and outreach to various stakeholders, including broker-dealers and investor groups. Based on the outcome of this risk-assessment process, OCIE conducts inspections of FINRA's major regulatory programs. OCIE also conducts oversight examinations of the examinations FINRA conducts of certain broker-dealers and municipal advisors. From its observations during all of these inspections and examinations, OCIE makes detailed recommendations to improve FINRA's programs, its risk assessment processes, and its future examinations.

MSRB

MSRB regulates the activities of broker-dealers that buy, sell, and underwrite municipal securities, and municipal advisors. MSRB establishes rules for municipal securities dealers and municipal advisors, supports market transparency by making municipal securities trade data and disclosure documents available, and conducts education and outreach regarding the municipal securities market. OCIE, along with FINRA, conducts examinations of registered firms to ensure compliance with MSRB rules. OCIE also applies a risk assessment process, similar to the one it uses to oversee FINRA, to identify areas to examine at MSRB. Examinations of MSRB evaluate the effectiveness of MSRB's policies, procedures, and controls.

CONCLUSION

These priorities reflect OCIE's assessment of certain risks, issues, and policy matters arising from market and regulatory developments, information gathered from examinations, and other sources, including tips, complaints, and referrals, and coordination with other Divisions and Offices at the SEC as well as other regulators. OCIE welcomes comments and suggestions regarding how it can better fulfill its mission to promote compliance, prevent fraud, identify and monitor risk, and inform SEC policy. Our contact information is available at <https://www.sec.gov/ocie>. If you suspect or observe activity that may violate the federal securities laws or otherwise operates to harm investors, please notify SEC Staff at <https://www.sec.gov/tcr>.



U.S. Securities and
Exchange Commission
100 F Street NE
Washington, DC 20549
SEC.gov

OCIE's 2020 Exam Priorities — Key Takeaways for Private Fund Managers

January 14, 2020

Last week, the SEC's Office of Compliance Inspections and Examinations released its 2020 Exam Priorities with a number of areas of interest to private fund managers. OCIE reported that it examined 15% of registered investment advisers (RIAs) during fiscal year 2019, down from approximately 17% of RIAs during FY 2018 but consistent with FY 2017's 15% coverage rate. The four-week government shutdown in January 2019 reduced exam activity last year, but we expect the numbers to trend upward in 2020.

The 2020 priorities include a number of new areas of note, although some areas (*e.g.*, conflicts, fees and expenses) appear year after year. Unlike last year's version, OCIE's 2020 priorities contain a section specifically addressing private fund managers, noting the following focus areas:

- Private fund managers advising different types of clients, including those that also manage a registered investment company with a similar investment strategy, or those that advise separately managed accounts side-by-side with private funds. These managers can expect a focus on potential conflicts of interest, allocation issues and fiduciary obligations involving different types of clients.
- Controls to prevent the misuse of material, non-public information (MNPI).
- Compliance risks involving conflicts of interest, such as "undisclosed or inadequately disclosed fees and expenses, and the use of RIA affiliates to provide services to clients."

Alternative Data

For the first time, OCIE has publicly identified alternative data as an exam priority, stating that "examinations will focus on firms' use of these data sets and technologies to interact with and provide services to investors, firms, and other service providers and assess the effectiveness of related compliance and control functions." Fund managers using alternative data should be prepared for questions regarding their diligence process for alternative data vendors, protections against receipt of personally identifiable information (PII), and potential MNPI considerations involving alternative data, among other issues.

Fiduciary Obligations

Following the SEC's recent Interpretation Regarding Standard of Conduct for Investment Advisers, OCIE has reiterated that it will continue to focus on whether advisers are complying with their fiduciary obligations to clients. Specifically, "whether RIAs provide advice in the best interests of their clients and eliminate, or at least expose through full and fair disclosure, all conflicts of interest which might incline an RIA, consciously or unconsciously, to render advice which is not disinterested." Key examples are fee and expense allocations and inadequately disclosed compensation arrangements. These areas and related potential conflicts of interest are typically on OCIE's list of priorities, and we expect them to be a continued focus in light of the SEC's recent interpretive guidance on fiduciary obligations.

New or Emerging Investment Strategies (e.g., ESG)

The 2020 priorities state that OCIE will have a particular interest in the accuracy and adequacy of disclosures provided by RIAs offering clients new types or emerging investment strategies, such as strategies focused on sustainable and responsible investing, or which incorporate environmental, social, and governance (ESG) criteria. We expect exams to focus on disclosures to potential investors, how ESG investments are defined internally and externally, and the internal process for monitoring those strategies.

Information Security

OCIE will continue to prioritize cyber and other information security risks across the entire examination program.

AML Programs

OCIE will continue to review managers' compliance with applicable anti-money laundering (AML) requirements, including whether entities are appropriately adapting their AML programs to address their particular situations and regulatory obligations.

Who's Up Next

Which advisers are most likely to be examined? As stated in the priorities, OCIE remains focused on examining firms that have never been examined or have not recently been examined, especially if the firm has substantially grown or expanded into new products. Because OCIE is focusing on conducting more (and more targeted) exams, the chances of undergoing an exam have remained high, but the scope of the exams may be narrower. The selection is data-driven, so if OCIE's data-crunchers believe that a manager exhibits characteristics falling within its priorities or other risk areas, then the chances of an exam will increase.



NATIONAL EXAM PROGRAM

RISK ALERT

By the Office of Compliance Inspections and Examinations*

October 31, 2018

Investment Adviser Compliance Issues Related to the Cash Solicitation Rule

Key Takeaway:
Advisers should review their practices and policies to ensure compliance with the Cash Solicitation Rule.

I. Introduction

The Office of Compliance Inspections and Examinations (“OCIE”) is issuing this Risk Alert to provide investment advisers, investors and other market participants with information concerning the most common deficiencies the staff has cited relating to Rule 206(4)-3 (the “Cash Solicitation Rule”) under the Investment Advisers Act of 1940 (the “Advisers Act”).¹ This Risk Alert includes observations by OCIE staff and is intended to assist investment advisers in identifying potential issues and adopting and implementing effective compliance programs.²

In general, investment advisers required to be registered under the Advisers Act (“advisers”) are prohibited from paying a cash fee, directly or indirectly, to any person who solicits clients for the adviser (a “solicitor”) unless the arrangement complies with a number of conditions.³ Among other things, the cash fee must be paid pursuant to a written agreement to which the adviser is a party (the “solicitation agreement”).⁴ The solicitor may not be a person subject to certain disqualifications specified in the Cash Solicitation Rule.

There are additional requirements when the solicitor is not a partner, officer, director or employee of the adviser or of an entity that controls, is controlled by, or is under common control with, the adviser (a “third-party solicitor”).⁵ The Cash Solicitation Rule imposes the

* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the “SEC” or the “Commission”) has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

¹ This Risk Alert reflects issues identified during a review of deficiency letters from investment adviser examinations completed during the past three years.

² The SEC has brought enforcement actions charging advisers with violations of the Cash Solicitation Rule. *See, e.g., In the Matter of Essex Fin. Servs., Inc.*, Advisers Act Rel. No. 4603 (Jan. 9, 2017) (settled order) (finding that adviser violated the Cash Solicitation Rule by paying a cash fee to a solicitor despite knowing that the solicited clients had not received the necessary disclosures).

³ Advisers Act Rule 206(4)-3.

⁴ A copy of the solicitation agreement must be retained by the adviser under Advisers Act Rule 204-2(a)(15).

⁵ Advisers are subject to narrower requirements under the Cash Solicitation Rule when (1) the solicitor is a partner, officer, director or employee of the adviser or of an entity that controls, is controlled by, or is under

following additional requirements when an adviser uses a third-party solicitor:

- (1) the solicitation agreement must contain certain specified provisions (e.g., a description of the solicitation activities and compensation to be received);
- (2) the solicitation agreement must require that, at the time of any solicitation activities, the solicitor provide the prospective client with a copy of (a) the adviser's brochure pursuant to Advisers Act Rule 204-3 ("adviser brochure") and (b) a separate, written disclosure document containing required information that highlights the solicitor's financial interest in the client's choice of an adviser (the "solicitor disclosure document");
- (3) the adviser must receive from the client, before or at the time of entering into any written or oral agreement with the client, a signed and dated acknowledgment that the client received the adviser brochure and the solicitor disclosure document ("client acknowledgement"); and
- (4) the adviser must make a bona fide effort to ascertain whether the solicitor has complied with the solicitation agreement, and must have a reasonable basis for believing that the solicitor has so complied.⁶

II. Most Frequent Compliance Issues Related to the Cash Solicitation Rule

Below are some of the most frequent deficiencies that OCIE staff has identified pertaining to the Cash Solicitation Rule.⁷

- *Solicitor disclosure documents.* OCIE staff observed advisers whose third-party solicitors did not provide solicitor disclosure documents to prospective clients or provided solicitor disclosure documents that did not contain all the information required by the Cash Solicitation Rule. For example, staff observed solicitor disclosure documents that did not:
 - Disclose the nature of the relationship, including any affiliation, between the solicitor and the adviser.
 - Contain the terms of the compensation arrangement between the adviser and the solicitor.
 - Specify the actual compensation terms agreed to in the solicitation agreement and instead used vague or hypothetical terms to describe the solicitor's compensation.

common control with, the adviser or (2) the cash fee is paid with respect to solicitation activities for the provision of impersonal advisory services only. Advisers Act Rule 206(4)-3(a)(2)(i)-(ii). This Risk Alert generally includes observations relating to an adviser's use of third-party solicitors subject to the broader requirements of the Cash Solicitation Rule.

⁶ Advisers Act Rule 206(4)-3(a)(2)(iii).

⁷ This Risk Alert does not address all deficiencies or weaknesses related to the Cash Solicitation Rule that have been identified by OCIE staff.

- Specify the additional solicitation cost the solicited client will be charged in addition to the advisory fee.
- *Client acknowledgements.* OCIE staff observed advisers that did not timely receive a signed and dated client acknowledgement of receipt of the adviser brochure and the solicitor disclosure document.⁸ Staff also observed advisers that received client acknowledgements, but such client acknowledgements were undated or dated after the clients had entered into an investment advisory contract.
- *Solicitation agreements.* OCIE staff observed advisers that paid cash fees to a solicitor without a solicitation agreement in effect or pursuant to an agreement that did not contain certain specific provisions.⁹ For example, staff observed solicitation agreements with third-party solicitors that did not:
 - Contain an undertaking by the solicitor to perform its duties under the solicitation agreement in a manner consistent with the instructions of the adviser.
 - Describe the solicitor's activities and the compensation to be paid.
 - Oblige solicitors to provide clients (including prospective clients) with a current copy of the adviser brochure and the solicitor disclosure document.
- *Bona fide efforts to ascertain solicitor compliance.* OCIE staff observed advisers that did not make a bona fide effort to ascertain whether third-party solicitors complied with solicitation agreements and appeared to not have a reasonable basis for believing that the third-party solicitors so complied.¹⁰ For example, staff observed advisers that were unable to describe any efforts they took to confirm compliance with solicitation agreements.

OCIE also observed advisers with similar conflicts that may implicate other provisions of the Advisers Act, such as an adviser's fiduciary duty under Sections 206(1) and 206(2). For example, OCIE observed advisers that recommended service providers to clients in exchange for client referrals without full and fair disclosure of the conflicts of interest.

III. Conclusion

The examinations within the scope of this review resulted in a range of actions. In response to the staff's observations, some advisers elected to amend their disclosure documents and solicitation agreements, revise their compliance policies and procedures, or otherwise change their practices regarding the Cash Solicitation Rule.

⁸ Advisers Act Rule 206(4)-3(a)(2)(iii)(B).

⁹ Advisers Act Rule 206(4)-3(a)(2)(iii)(A).

¹⁰ Advisers Act Rule 206(4)-3(a)(2)(iii)(C).

In sharing the information in this Risk Alert, OCIE encourages advisers to review their practices, policies, and procedures in these areas and to promote improvements in adviser compliance programs.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.



NATIONAL EXAM PROGRAM

RISK ALERT

By the Office of Compliance Inspections and Examinations*

Observations from Investment Adviser Examinations Relating to Electronic Messaging

I. Introduction

Key takeaway. OCIE encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with applicable regulatory requirements.

The Office of Compliance Inspections and Examinations (“OCIE”) conducted a limited-scope examination initiative of registered investment advisers (“advisers”) designed to obtain an understanding of the various forms of electronic messaging used by advisers and their personnel, the risks of such use, and the challenges in complying with certain provisions of the Investment Advisers Act of 1940 (“Advisers Act”). OCIE conducted this initiative because it noticed an increasing use of various types of electronic messaging by adviser personnel for business-related communications.¹

The purpose of this Risk Alert is to remind advisers of their obligations when their personnel use electronic messaging and to help advisers improve their systems, policies, and procedures by sharing the staff’s observations from these examinations.

II. Relevant Regulation

Advisers Act Rule 204-2 (“Books and Records Rule”) requires advisers to make and keep certain books and records relating to their investment advisory business, including typical accounting and other business records as required by the Commission. For example, Rule 204-2(a)(7) requires advisers to make and keep “[o]riginals of all written communications received and copies of all written communications sent by such investment adviser relating to (i) any recommendation made or proposed to be made and any advice given or proposed to be given, (ii) any receipt, disbursement or delivery of funds or securities, (iii) the placing or execution of any order to purchase or sell any security, or (iv) the performance or rate of return of any or all managed accounts or securities recommendations,” subject to certain limited exceptions.

Additionally, Rule 204-2(a)(11) requires advisers to make and keep a copy of each notice,

* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the “SEC” or the “Commission”) has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

¹ Numerous articles also have been written on electronic messaging trends and the compliance challenges that they may pose. See e.g., Jackie Noblett, *SMH: Texting, Chat Continue to Vex Compliance Depts.*, IGNITES (June 2, 2017) and Jason Wallace, *Text Messaging: The Communication Risk Compliance Fears Most – Survey*, REGULATORY INTELLIGENCE (May 26, 2017).

circular, advertisement, newspaper article, investment letter, bulletin or other communication that the investment adviser circulates or distributes, directly or indirectly, to ten or more persons. The Commission has stated that, “regardless of whether information is delivered in paper or electronic form, broker-dealers and investment advisers must reasonably supervise firm personnel with a view to preventing violations.”²

Advisers Act Rule 206(4)-7 (“Compliance Rule”) requires advisers to adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and rules thereunder.³ According to the Compliance Rule’s adopting release, each adviser should identify compliance factors creating risk exposures for the firm and its clients in light of the adviser’s particular operations, and then design policies and procedures that address those risks.⁴ The Commission stated that an adviser’s policies and procedures should address, to the extent relevant to the adviser, “[t]he accurate creation of required records and their maintenance in a manner that secures them from unauthorized alteration or use and protects them from untimely destruction,” among other things.⁵ The Compliance Rule also requires an adviser to review, no less frequently than annually, the adequacy of the adviser’s compliance policies and procedures and the effectiveness of their implementation.

As discussed below, a number of changes in the way mobile and personally owned devices are used pose challenges for advisers in meeting their obligations under the Books and Records Rule and the Compliance Rule.⁶ These changes include the increasing use of social media, texting, and other types of electronic messaging apps, and the pervasive use of mobile and personally owned devices for business purposes.

III. Scope of Electronic Messaging Covered by the Examinations

OCIE’s examinations surveyed firms to learn the types of electronic messaging used by firms and their personnel,⁷ and reviewed firms’ policies and procedures to understand how advisers were addressing the risks presented by evolving forms of electronic communication. For purposes of this initiative, “electronic messaging” or “electronic communication” included

² *Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information*, Advisers Act Rel. No. 1562 (May 9, 1996), available at <https://www.sec.gov/rules/interp/33-7288.txt>.

³ Advisers Act Rule 206(4)-7(a).

⁴ *Compliance Programs of Investment Companies and Investment Advisers*, Advisers Act Release No. 2204 (Dec. 17, 2003) at Section II.A.1., available at <http://www.sec.gov/rules/final/ia-2204.htm>.

⁵ See *id.* at n.19 and accompanying text.

⁶ This Risk Alert is not intended to be a comprehensive overview of all applicable regulatory requirements. The use of electronic messaging may implicate regulations beyond those specifically discussed in this Risk Alert.

⁷ Adviser legal and regulatory requirements generally cover persons associated with an adviser, which can include many types of advisory personnel – such as employees, independent contractors, and investment adviser representatives. For purposes of this Risk Alert, the terms “personnel,” “employees,” and “representatives” are used interchangeably and include independent contractors.

written business communications conveyed electronically using, for example, text/SMS messaging, instant messaging, personal email, and personal or private messaging. OCIE included communications when conducted on the adviser's systems or third-party applications ("apps") or platforms or sent using the adviser's computers, mobile devices issued by advisory firms, or personally owned computers or mobile devices used by the adviser's personnel for the adviser's business.

The staff specifically excluded email use on advisers' systems from this review because firms have had decades of experience complying with regulatory requirements with respect to firm email, and it often does not pose similar challenges as other electronic communication methods because it occurs on firm systems and not on third-party apps or platforms.

IV. Summary of Examination Observations

OCIE's examination initiative focused on whether and to what extent advisers complied with the Books and Records Rule and adopted and implemented policies and procedures as required by the Compliance Rule. During the course of the initiative, the staff observed a range of practices with respect to electronic communications, including advisers that did not conduct any testing or monitoring to ensure compliance with firm policies and procedures. The staff observed and identified the following examples of practices⁸ that the staff believes may assist advisers in meeting their record retention obligations under the Books and Records Rule and their implementation and design of policies and procedures under the Compliance Rule:

Policies and Procedures

- Permitting only those forms of electronic communication for business purposes that the adviser determines can be used in compliance with the books and records requirements of the Advisers Act.
- Specifically prohibiting business use of apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up.
- In the event that an employee receives an electronic message using a form of communication prohibited by the firm for business purposes, requiring in firm procedures that the employee move those messages to another electronic system that the adviser determines can be used in compliance with its books and records obligations, and including specific instructions to employees on how to do so.
- Where advisers permit the use of personally owned mobile devices for business purposes, adopting and implementing policies and procedures addressing such use

⁸ This Risk Alert is not intended to be a comprehensive list of practices for a firm to meet its regulatory obligations, but rather to provide a sample of practices staff observed that may be helpful to advisers assessing their compliance policies and procedures addressing electronic messaging, including with respect to recordkeeping, supervision, or cybersecurity.

with respect to, for example, social media, instant messaging, texting, personal email, personal websites, and information security.

- If advisers permit their personnel to use social media, personal email accounts, or personal websites for business purposes, adopting and implementing policies and procedures for the monitoring, review, and retention of such electronic communications.
- Including a statement in policies and procedures informing employees that violations may result in discipline or dismissal.

Employee Training and Attestations

- Requiring personnel to complete training on the adviser's policies and procedures regarding prohibitions and limitations placed on the use of electronic messaging and electronic apps and the adviser's disciplinary consequences of violating these procedures.
- Obtaining attestations from personnel at the commencement of employment with the adviser and regularly thereafter that employees (i) have completed all of the required training on electronic messaging, (ii) have complied with all such requirements, and (iii) commit to do so in the future.
- Providing regular reminders to employees of what is permitted and prohibited under the adviser's policies and procedures with respect to electronic messaging.
- Soliciting feedback from personnel as to what forms of messaging are requested by clients and service providers in order for the adviser to assess their risks and how those forms of communication may be incorporated into the adviser's policies.

Supervisory Review

- For advisers that permit use of social media, personal email, or personal websites for business purposes, contracting with software vendors to (i) monitor the social media posts, emails, or websites, (ii) archive such business communications to ensure compliance with record retention rules, and (iii) ensure that they have the capability to identify any changes to content and compare postings to a lexicon of key words and phrases.
- Regularly reviewing popular social media sites to identify if employees are using the media in a way not permitted by the adviser's policies. Such policies included prohibitions on using personal social media for business purposes or using it outside of the vendor services the adviser uses for monitoring and record retention.
- Running regular Internet searches or setting up automated alerts to notify the adviser when an employee's name or the adviser's name appears on a website to identify potentially unauthorized advisory business being conducted online.

- Establishing a reporting program or other confidential means by which employees can report concerns about a colleague’s electronic messaging, website, or use of social media for business communications. Particularly with respect to social media, colleagues may be “connected” or “friends” with each other and see questionable or impermissible posts before compliance staff notes them during any monitoring.

Control over Devices

- Requiring employees to obtain prior approval from the adviser’s information technology or compliance staff before they are able to access firm email servers or other business applications from personally owned devices. This may help advisers understand each employee’s use of mobile devices to engage in advisory activities.
- Loading certain security apps or other software on company-issued or personally owned devices prior to allowing them to be used for business communications. Software is available that enables advisers to (i) “push” mandatory cybersecurity patches to the devices to better protect the devices from hacking or malware, (ii) monitor for prohibited apps, and (iii) “wipe” the device of all locally stored information if the device were lost or stolen.
- Allowing employees to access the adviser’s email servers or other business applications only by virtual private networks or other security apps to segregate remote activity to help protect the adviser’s servers from hackers or malware.

V. Conclusion

In sharing its observations from this examination initiative, OCIE encourages advisers to review their risks, practices, policies, and procedures regarding electronic messaging and to consider any improvements to their compliance programs that would help them comply with their regulatory requirements. OCIE also encourages advisers to stay abreast of evolving technology and how they are meeting their regulatory requirements while utilizing new technology.

While this initiative was limited to examinations of investment advisers and this Risk Alert only references regulatory provisions under the Advisers Act, other types of regulated financial services entities may face similar challenges with new communication tools and methods.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm’s business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.



RISK ALERT

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

April 16, 2019

Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies

Key Takeaway: Through sharing some of the Regulation S-P compliance issues it observed, OCIE encourages registrants to review their written policies and procedures, including implementation of those policies and procedures, to ensure compliance with the relevant regulatory requirements.

I. Introduction

The Office of Compliance Inspections and Examinations (“OCIE”)* is providing a list of compliance issues related to Regulation S-P, the primary SEC rule regarding privacy notices and safeguard policies of investment advisers and broker-dealers.¹ These issues were identified in recent examinations of SEC-registered investment advisers (“advisers”) and brokers and dealers (“broker-dealers,” and together with advisers, “registrants” or “firms”).² The information in this Risk Alert is intended to assist advisers and broker-dealers in providing compliant privacy and opt-out notices, and in adopting and implementing effective policies and procedures for safeguarding customer records and information, under Regulation S-P.³

Privacy and Opt-Out Notices

Regulation S-P, among other things, requires a registrant to: (1) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices generally no later than when it establishes a customer relationship (“Initial

* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (“SEC”) has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

¹ See 17 CFR Part 248, Subpart A, and Appendix A to Subpart A. See also [Privacy of Consumer Financial Information \(Regulation S-P\)](#), Release Nos. 34-42974, IC-24543, IA-1883 (June 22, 2000) (adopting rules implementing the privacy provisions of Subtitle A of Title V of the Gramm- Leach-Bliley Act (“GLBA”) with respect to financial institutions regulated by the SEC); [Disposal of Consumer Report Information](#), Release Nos. 34-50781, IA-2332, IC-26685 (December 2, 2004) (adding rule requiring proper disposal of consumer report information (17 CFR 248.30(b), “Disposal Rule”) and amending rule requiring policies and procedures reasonably designed to safeguard customer records and information (17 CFR 248.30(a), “Safeguards Rule”) to require written policies and procedures); [Final Model Privacy Form under the Gramm-Leach-Bliley Act](#), Release Nos. 34-61003, IA-2950, IC-28997 (November 16, 2009) (adding model privacy form and instructions in appendix).

² This Risk Alert reflects issues identified in deficiency letters from broker-dealer and adviser exams completed during the past two years. This Risk Alert does not discuss all types of deficiencies or weaknesses related to Regulation S-P that have been identified by staff.

³ This Risk Alert does not discuss all requirements of Regulation S-P.

Privacy Notice”),⁴ (2) provide a clear and conspicuous notice to its customers that accurately reflects its privacy policies and practices not less than annually during the continuation of the customer relationship (“Annual Privacy Notice,”⁵ and together with the Initial Privacy Notice, “Privacy Notices”),⁶ and (3) deliver a clear and conspicuous notice to its customers that accurately explains the right to opt out of some disclosures of non-public personal information about the customer to nonaffiliated third parties (“Opt-Out Notice”).⁷ Regulation S-P describes the information that must be included in Privacy Notices, including the categories of nonpublic personal information that the registrant collects and discloses, and in Opt-Out Notices.⁸

Written Safeguarding Policies and Procedures to Safeguard Customer Information

The Safeguards Rule of Regulation S-P requires registrants to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information.⁹ These written policies and procedures must be reasonably designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of customer records and information, and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

II. Most Frequent Regulation S-P Compliance Issues

Below are examples of the most common deficiencies or weaknesses identified by OCIE staff in connection with the Safeguards Rule.

- A. *Privacy and Opt-Out Notices.* OCIE staff observed registrants that did not provide Initial Privacy Notices, Annual Privacy Notices and Opt-Out Notices to their customers. When such notices were provided to customers, the notices did not accurately reflect firms’ policies and procedures. The staff also noted Privacy Notices that did not provide notice

⁴ 17 CFR 248.4. Regulation S-P defines “customer” to mean a consumer that has a customer relationship with a financial institution, and a “customer relationship” as a continuing relationship between a consumer and a financial institution and includes an individual who has a brokerage account with a broker-dealer or an advisory contract with an investment adviser (whether written or oral). 17 CFR 248.3(j)-(k). As used in this Risk Alert, “customer” refers to brokerage customers and advisory clients as applicable.

⁵ 17 CFR 248.5. Section 75001 of the Fixing America’s Surface Transportation Act, Pub. L. No. 114-94, 129 Stat. 1312 (2016), (“FAST Act”) amended the GLBA by adding subsection 503(f) to provide an exception to the Annual Privacy Notice requirement. Under this exception, a financial institution is not required to provide an Annual Privacy Notice if the financial institution (1) does not share nonpublic personal information about the customer except for certain purposes that do not trigger the customer’s statutory right to opt out and (2) has not changed its policies and practices with regard to disclosing nonpublic personal information from the policies and practices that were disclosed in the most recent Privacy Notice.

⁶ The SEC has adopted a model form to satisfy Privacy Notice disclosure requirements. Use of the form provides a “safe harbor” for the required disclosures under Regulation S-P. 17 CFR 248.2. *See also* [Final Model Privacy Form under the Gramm-Leach-Bliley Act](#), *supra* note 1.

⁷ 17 CFR 248.7. Under the exceptions in 17 CFR 248.13, 248.14 and 248.15, however, an Opt-Out Notice is not required if the registrant shares nonpublic personal information with a non-affiliated third party for certain purposes.

⁸ 17 CFR 248.6, 248.7.

⁹ 17 CFR 248.30(a).

to customers of their right to opt out of the registrant sharing their nonpublic personal information with nonaffiliated third parties.

- B. *Lack of policies and procedures.* OCIE staff observed registrants that did not have written policies and procedures as required under the Safeguards Rule. For example, firms had documents that restated the Safeguards Rule but did not include policies and procedures related to administrative, technical, and physical safeguards. The staff observed written policies and procedures that contained numerous blank spaces designed to be filled in by registrants. There were also firms with policies that addressed the delivery and content of a Privacy Notice, but did not contain any written policies and procedures required by the Safeguards Rule.
- C. *Policies not implemented or not reasonably designed to safeguard customer records and information.* OCIE staff observed registrants with written policies and procedures that did not appear implemented or reasonably designed to (1) ensure the security and confidentiality of customer records and information, (2) protect against anticipated threats or hazards to the security or integrity of customer records and information, and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to customers. For example, staff observed:
- Personal devices. Policies and procedures that did not appear reasonably designed to safeguard customer information on personal devices. For example, staff observed registrants' employees who regularly stored and maintained customer information on their personal laptops, but the registrants' policies and procedures did not address how these devices were to be properly configured to safeguard the customer information.
 - Electronic communications. Policies and procedures that did not address the inclusion of customer personally identifiable information ("PII") in electronic communications. For example, staff observed registrants that did not appear to have policies and procedures reasonably designed to prevent employees from regularly sending unencrypted emails to customers containing PII.
 - Training and monitoring. Policies and procedures that required customer information to be encrypted, password-protected, and transmitted using only registrant-approved methods were not reasonably designed because employees were not provided adequate training on these methods and the firm failed to monitor if the policies were being followed by employees.
 - Unsecure networks. Policies and procedures that did not prohibit employees from sending customer PII to unsecure locations outside of the registrants' networks.
 - Outside vendors. Registrants failed to follow their own policies and procedures regarding outside vendors. For example, staff observed registrants that failed to require outside vendors to contractually agree to keep customers' PII confidential, even though such agreements were mandated by the registrant's policies and procedures.

- PII inventory. Policies and procedures that did not identify all systems on which the registrant maintained customer PII. Without an inventory of all such systems, registrants may be unaware of the categories of customer PII that they maintain, which could limit their ability to adopt reasonably designed policies and procedures and adequately safeguard customer information.
- Incident response plans. Written incident response plans that did not address important areas, such as role assignments for implementing the plan, actions required to address a cybersecurity incident, and assessments of system vulnerabilities.¹⁰
- Unsecure physical locations. Customer PII that was stored in unsecure physical locations, such as in unlocked file cabinets in open offices.
- Login credentials. Customer login credentials that had been disseminated to more employees than permitted under firms' policies and procedures.
- Departed employees. Instances where former employees of firms retained access rights after their departure and therefore could access restricted customer information.

III. Conclusion

In response to these observations, many of the registrants modified their written policies and procedures to mitigate the issues identified by OCIE staff. OCIE encourages registrants to review their written policies and procedures, including implementation of those policies and procedures, to ensure that they are compliant with Regulation S-P.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

¹⁰ For a discussion of related cybersecurity compliance issues, please see the OCIE Risk Alert [Observations from Cybersecurity Examinations](#), August 7, 2017.



RISK ALERT

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

May 23, 2019

Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features

Key Takeaway: *This Risk Alert highlights risks associated with the storage of electronic customer records and information by broker-dealers and investment advisers in the cloud and on other types of network storage solutions.*

I. Introduction

During recent examinations, the Office of Compliance Inspections and Examinations (“OCIE”)* identified security risks associated with the storage of electronic customer records and information by broker-dealers and investment advisers in various network storage solutions, including those leveraging cloud-based storage.¹ Although the majority of these network storage solutions offered encryption, password protection, and other security features designed to prevent unauthorized access, examiners observed that firms did not always use the available security features. Weak or misconfigured security settings on a network storage device could result in unauthorized access to information stored on the device.

II. Summary of Examination Observations

OCIE staff has observed firms storing electronic customer records and information using various types of storage solutions, including cloud-based storage. During examinations, OCIE staff identified the following concerns that may raise compliance issues under Regulations S-P and S-ID:²

- *Misconfigured network storage solutions.* In some cases, firms did not adequately configure the security settings on their network storage solution to protect against unauthorized access. In addition, some firms did not have policies and procedures addressing the security configuration of

* The views expressed herein are those of the staff of OCIE. The Securities and Exchange Commission (the “SEC” or the “Commission”) has expressed no view on the contents of this Risk Alert. This document was prepared by OCIE staff and is not legal advice.

¹ Cloud storage refers to the electronic storage of information on infrastructure owned and operated by a hosting company or service provider. See, e.g., [The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-145 \(September 2011\)](#).

² The Safeguards Rule of Regulation S-P requires every broker-dealer and investment adviser registered with the Commission to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. 17 C.F.R. 248.30(a).

The Identity Theft Red Flags Rule of Regulation S-ID requires broker-dealers and investment advisers registered or required to be registered with the Commission to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. 17 C.F.R. 248.201. A covered account includes an account that a broker-dealer or investment adviser offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions. 17 C.F.R. 201(b)(3).

their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.

- *Inadequate oversight of vendor-provided network storage solutions.* In some cases, firms did not ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on vendor-provided network storage solutions were configured in accordance with the firm's standards.
- *Insufficient data classification policies and procedures.* In some cases, firms' policies and procedures did not identify the different types of data stored electronically by the firm and the appropriate controls for each type of data.

III. Examples of Effective Practices

The implementation of a configuration management program that includes policies and procedures governing data classification, vendor oversight, and security features will help to mitigate the risks incurred when implementing on-premise or cloud-based network storage solutions. During examinations, OCIE staff has observed several features of effective configuration management programs, data classification procedures, and vendor management programs, including:

- Policies and procedures designed to support the initial installation, on-going maintenance, and regular review of the network storage solution;
- Guidelines for security controls and baseline security configuration standards to ensure that each network solution is configured properly; and
- Vendor management policies and procedures that include, among other things, regular implementation of software patches and hardware updates followed by reviews to ensure that those patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration.

IV. Conclusion

In sharing these observations, OCIE encourages registered broker-dealers and investment advisers to review their practices, policies, and procedures with respect to the storage of electronic customer information and to consider whether any improvements are necessary. OCIE also encourages firms to actively oversee any vendors they may be using for network storage to determine whether the service provided by the vendor is sufficient to enable the firm to meet its regulatory responsibilities.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.



RISK ALERT

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

July 23, 2019

Observations from Examinations of Investment Advisers: Compliance, Supervision, and Disclosure of Conflicts of Interest

OCIE encourages advisers, when designing and implementing their compliance and supervision frameworks, to consider the risks presented by hiring and employing supervised persons with disciplinary histories and adopt policies and procedures to address those risks.

I. Introduction

As part of the Office of Compliance Inspections and Examination's ("OCIE") focus on protecting retail investors, the staff conducted a series of examinations to assess the oversight practices of SEC-registered investment advisers ("advisers") that previously employed, or currently employ, any individual with a history of disciplinary events ("Supervision Initiative" or "Initiative").¹

The staff conducted over 50 examinations of advisers in 2017 as part of this Initiative. The advisers examined collectively managed approximately \$50 billion in assets for nearly 220,000 clients, the vast majority of whom were retail investors. Advisers were identified for examination through a review of information about disciplinary events and other legal actions involving supervised persons of the adviser, including legal actions that are not required to be reported on

Form ADV (e.g., private civil actions).²

The purpose of this Risk Alert is to raise awareness of certain compliance issues that OCIE observed by sharing the staff's observations from these examinations.

II. Relevant Regulations

The Supervision Initiative focused on advisers' practices in certain areas, including:

¹ See [NEP Risk Alert: Examinations of Supervision Practices At Registered Investment Advisers](#) (Sept. 12, 2016). For purposes of the Supervision Initiative, and as referenced in this Risk Alert, "supervised persons" include principals and officers of the adviser, and other individuals performing services on behalf of the adviser (other than clerical), regardless of whether these individuals are independent contractors or employees of the adviser. See also Investment Advisers Act of 1940 ("Advisers Act") Section 202(a) (25) (defining "supervised person").

² See Form ADV, Part 2A, Item 9 and Part 2B, Item 3 (Disciplinary Information). All registered advisers must promptly disclose any legal or disciplinary events that would be material to a client's or a prospective client's evaluation of the adviser's integrity or its ability to meet its commitments to clients. See also Advisers Act Rules 204-3(b) (4) and 204(2)(a)(14)(iii).

- *Compliance programs and supervisory oversight practices.* The staff reviewed whether compliance policies and procedures were reasonably designed to detect and prevent violations of the Advisers Act by the firm and its supervised persons, particularly those policies and procedures covering the activities of certain previously-disciplined individuals.³
- *Disclosures.* The staff focused on whether disclosures in public statements or documents (e.g., marketing materials) and filings were full and fair, included all material facts, and were not misleading.⁴ Particular emphasis was placed on reviewing disclosures in these materials related to previously-disciplined individuals and their prior disciplinary events.⁵
- *Conflicts of interest.* The staff assessed whether the adviser identified, addressed, and fully and fairly disclosed all material conflicts of interest that could affect the advisory relationship, particularly those conflicts dealing with compensation arrangements and account management.⁶

The examinations did not focus solely on supervisory practices as they relate to the individuals with prior disciplinary histories. Rather, due to the importance that supervisory practices have in setting a strong “tone at the top” and compliance culture, the staff reviewed the advisers’ supervisory practices firm-wide.

III. Staff Observations

The Initiative identified a variety of observed deficiencies across a range of topics. Nearly all of the examined advisers received deficiency letters. The vast majority of these deficiencies relate to compliance issues, but many relate to disclosure issues, including undisclosed conflicts of interest.

³ Advisers Act Rule 206(4)-7. Section 203(e)(6) of the Advisers Act also highlights that establishing supervisory procedures reasonably designed to prevent and detect such violations and following these procedures are important steps an adviser should take in supervising persons subject to its supervision. The Commission has brought enforcement actions against advisers that did not adopt or implement any policies or procedures regarding their supervision of certain personnel. See, e.g., [In re James T Budden and Alexander Budden](#), Advisers Act Release No. 4225 (Oct. 13, 2015) (settled).

⁴ An adviser’s obligation as a fiduciary is enforceable through Advisers Act Section 206. As fiduciaries, advisers must provide full and fair disclosure of all material facts to their clients and prospective clients. Also, it is unlawful for advisers to make untrue statements or omit any material facts in applications or reports filed with the Commission (Advisers Act Section 207) or to have advertising (as defined in Advisers Act Rule 206(4)-1) that is false or misleading or that contains any untrue statement of a material fact.

⁵ See, e.g., [SEC v. Capital Gains Research Bureau, Inc.](#), 375 U.S. 180 (1963) and [Amendments to Form ADV](#), Advisers Act Release No. 3060 (Jul. 28, 2010) (“as a fiduciary, an adviser has an ongoing obligation to inform its clients of any material information that could affect the advisory relationship”). See also [General Instruction 3 to Form ADV](#), which states that “[u]nder federal and state law, [an adviser is] a fiduciary and must make full disclosure to [its] clients of all material facts relating to the advisory relationship.”

⁶ Advisers Act Section 206. Also, [General Instructions to Form ADV](#), such as General Instruction 3, state that an adviser’s disclosure obligation “...requires that [the adviser] provide the client with sufficiently specific facts so that the client is able to understand the conflicts of interest [the adviser has] and the business practices in which [the adviser] engage[s], and can give informed consent to such conflicts or practices or reject them.”

A. Staff Observations Specific to Disciplinary Histories

Some of the staff's observations related to advisers' oversight of supervised persons with disciplinary histories are discussed below.

- *Full and Fair Disclosure.* The staff observed that nearly half of the disclosure-related deficiencies of the advisers examined were due to the firms providing inadequate information regarding disciplinary events.⁷ For example, advisers:
 - Omitted material disclosures regarding disciplinary histories of certain supervised persons or the adviser itself. Often the disciplinary omissions related to supervised persons occurred because the advisers solely relied on these supervised persons to self-report to the firms information about their required disclosures.
 - Included incomplete, confusing, or misleading information regarding disciplinary events. For example, they did not, as applicable: include the total number of events, the date for each event, the allegations, or whether the supervised persons were found to be at fault (i.e., whether fines, judgments or awards, or other disciplinary sanctions were imposed).⁸
 - Did not timely update and deliver disclosure documents to clients, such as updating Form ADV for new disciplinary events of supervised persons reported on CRD (e.g., Form U5s).⁹
- *Effective compliance programs.* The staff observed that many advisers did not adopt and implement compliance policies and procedures that address the risks associated with hiring and employing individuals with prior disciplinary histories. For example, advisers did not have processes reasonably designed to identify:
 - Whether the supervised persons' self-attestations regarding disciplinary events completely and accurately described those events. For example, some self-attestations contained information that did not fully or clearly describe the disciplinary events.
 - Whether the supervised persons' self-attestations that they were not the subject of reportable events or recent bankruptcies was in fact the case. For example, some

⁷ All registered advisers must promptly disclose in Form ADV certain legal or disciplinary events that would be material to a client's or a prospective client's evaluation of the adviser's integrity or its ability to meet its commitments to clients. See [Amendments to Form ADV](#), Advisers Act Release No. 3060 (Jul. 28, 2010). See also generally, [Commission Interpretation Regarding Standard of Conduct for Investment Advisers](#), Advisers Act Release 5248 (June 5, 2019).

⁸ See [Form ADV](#), Item 11 and Criminal Disclosure Reporting Page (DRP), which requires advisers to report details regarding certain disciplinary events.

⁹ See [General Instructions to Form ADV](#), which specifies that an adviser must promptly file an "other-than-annual amendment" to its Form ADV when certain information becomes inaccurate in any way, including reportable disciplinary events. CRD (Central Registration Depository) is a database maintained by FINRA. It is used to store and maintain information on registered broker-dealers and their associated individuals. Many supervised persons of advisers are representatives of both broker-dealers and advisers.

supervised persons reported incorrectly to the adviser that they were not the subject of any reportable events during the reporting period or did not report information regarding recent bankruptcies.

B. Additional Staff Observations

The staff reviewed advisers' firm-wide practices and observed issues that were not necessarily attributed directly to the firms' hiring and supervision of individuals with disciplinary histories. While some of these deficiencies are commonly identified in OCIE examinations, they were frequently identified during the Supervision Initiative examinations.

Compliance and Supervision

- *Supervision.* The staff observed that many advisers did not adequately supervise or set appropriate standards of business conduct for their supervised persons. In these instances, advisers' policies and procedures did not sufficiently document the responsibilities of supervised persons or did not clearly outline the expectations for these individuals. Examples include practices where the adviser did not:
 - Oversee whether fees charged by supervised persons were disclosed or assess whether the services clients paid for were performed. At some of these advisers, the staff observed instances in which clients paid for certain services they did not receive or were charged undisclosed fees.
 - Have advertising policies and procedures that provided sufficiently specific guidance to supervised persons who prepared their own advertising materials and websites. At these advisers, the staff observed the dissemination of advertisements that did not comply with the requirements of the advertising rule.¹⁰
 - Include reviewing activities of supervised persons, including supervised persons with disciplinary histories, working from remote locations as part of its monitoring activities. In many instances, staff observed that, unbeknownst to the advisers, geographically dispersed supervised persons were operating in a self-directed manner that was not consistent with the advisers' policies and procedures.
- *Oversight.* The staff observed that many advisers did not confirm that supervised persons identified as responsible for performing certain compliance policies and procedures were executing their duties, as prescribed. These advisers may have had policies and procedures that clearly assigned the individuals who were responsible for performing particular duties, but the firms did not implement them so that these individuals performed the duties that were assigned to them, or did not document that these duties were performed according to the advisers' policies and procedures. In some instances, the duties included key regulatory and business responsibilities for advisers managing investor assets, such as:

¹⁰ Advisers Act Rule 206(4)-1.

- Monitoring the appropriateness of client account types. For example, although outlined within the advisers' policies and procedures, the firms did not review whether at account opening the type of account selected was appropriate (e.g., wrap fee versus separately managed account), document that an assessment of the type of account took place, or document the factors considered in making these assessments.
 - Maintaining true, accurate, and current books and records, including those necessary to provide investment supervisory or management services to clients (e.g., maintaining a list of all accounts in which the adviser is vested with discretionary authority), to determine the financial standing of the firm, or to identify individuals with access to sensitive information.
- *Compliance policies and procedures.* The staff observed that several advisers had adopted policies and procedures that were inconsistent with their actual business practices and disclosures. Areas of inconsistent compliance practices most frequently cited by the staff involved those addressing commissions, fees, and expenses (e.g., solicitation fees, management fees, compensation related to hiring personnel, and oversight of firm compensation practices, including such practices within branch offices).
- *Annual compliance reviews.* The staff observed that advisers' annual reviews were insufficient because the firms did not take steps to adequately document the reviews and appropriately assess the risk areas applicable to the firms, or identify certain risks at all.

Disclosure of Conflicts of Interest

- *Compensation arrangements.* The staff observed that several advisers had undisclosed compensation arrangements, which resulted in conflicts of interests that could have impacted the impartiality of the advice the supervised persons gave to their clients. For example, some of these advisers did not disclose that:
 - Forgivable loans were made to the advisers or their supervised persons, the terms of which were contingent upon certain client-based incentives that may have unduly influenced the investment decision-making process, resulted in higher fees and expenses for the affected clients, or both.
 - Supervised persons were required to incur all transaction-based charges associated with executing client transactions, which created incentives for the supervised persons to trade less frequently on behalf of their clients.

IV. Staff Observations on Ways to Improve Compliance

Some of the compliance and supervisory policies and procedures the staff observed at certain advisers may help other firms address the weaknesses discussed above. For example, advisers that hire or employ supervised persons with disciplinary histories may want to consider, among other things:

- *Adopting written policies and procedures that specifically address what must occur prior to hiring supervised persons that have reported to the adviser disciplinary events.* Most of the examined advisers that had recently hired supervised persons that had reported to the adviser disciplinary histories had written policies and procedures specifically addressing what to do before hiring such individuals. The staff observed that, almost all of the firms' written policies and procedures required investigations of the disciplinary events and several also required ascertaining whether barred individuals were eligible to reapply for their licenses.
- *Enhancing due diligence practices associated with hiring supervised persons to identify disciplinary events.* The examined advisers utilized a wide array of due diligence measures as part of their hiring processes. The staff observed that, while the advisers' practices varied, in addition to the practices noted above, for firms with written hiring policies and procedures, these procedures more consistently included conducting background checks (e.g., the firms confirmed employment histories, disciplinary records, financial background and credit information), conducting internet and social media searches, fingerprinting personnel, utilizing third parties to research potential new hires, contacting personal references, and verifying educational claims. In addition, some advisers:
 - Requested that potential new hires provide the firm with copies of their Form U5s, when applicable.
 - Reviewed new hires' Form U5 filings 30 or more days after they are hired (this type of procedure may identify termination notices the new hire did not disclose that were filed after the hiring decision was made), when applicable.
 - Initially checked CRD/IARD for supervised persons' filings and re-checked the filing information after a designated period of time, such as three months later.
- *Establishing heightened supervision practices when overseeing supervised persons with certain disciplinary histories.* The staff observed that many of the advisers had not adopted supervision practices or compliance procedures that addressed the risks associated with employing supervised persons with prior disciplinary histories (e.g., disciplinary histories relating to misappropriation, unauthorized trading, forgery, bribery, and making unsuitable recommendations). However, the examined advisers with written policies and procedures specifically addressing the oversight of supervised persons with disciplinary histories were far more likely to identify misconduct by supervised persons than advisers without these written protocols.
- *Adopting written policies and procedures addressing client complaints related to supervised persons.* The staff observed that advisers with written policies and procedures addressing client complaints related to their supervised persons were more likely to have reported the receipt of at least one complaint related to their supervised persons. In addition, these advisers were consistently more likely to escalate matters of concern raised in these complaints than advisers without written protocols.

- *Including oversight of persons operating out of remote offices in compliance and supervisory programs, particularly when supervised persons with disciplinary histories are located in branch or remote offices.*

V. Conclusion

The examinations within the scope of this review resulted in a range of actions. In response to the staff's observations, some advisers elected to amend disclosures, revise compliance policies and procedures, or change other practices. OCIE encourages advisers, when designing and implementing their compliance and supervision frameworks, to consider the risks presented by, as well as the disclosure requirements triggered by, the hiring and employing of supervised persons with disciplinary histories and adopt policies and procedures to address those risks and disclosure requirements.

In sharing the information in this Risk Alert, OCIE is encouraging advisers to reflect upon their practices, policies, and procedures and to consider ways that they may improve their supervisory practices and compliance programs.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.



RISK ALERT

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

September 4, 2019

Investment Adviser Principal and Agency Cross Trading Compliance Issues

In this Alert: *The most frequent principal trading and agency cross transaction compliance issues identified by OCIE staff in examinations of advisers.*

I. Introduction

This Risk Alert provides an overview of the most common compliance issues identified by the Office of Compliance Inspections and Examinations (“OCIE”) * related to principal trading and agency cross transactions under Section 206(3) of the Advisers Act,¹ which were identified in examinations of investment advisers.²

Section 206(3) - Principal Trades

Section 206(3) makes it unlawful for any investment adviser, directly or indirectly, acting as principal for his own account knowingly to (a) sell any security to a client or (b) purchase any security from a client (“principal trades”), without disclosing to such client in writing before the completion of such transaction the capacity in which the adviser is acting and obtaining the consent of the client to such transaction. Section 206(3) requires an adviser entering into a principal trade with a client to satisfy these disclosure and consent requirements on a transaction-by-transaction basis – blanket disclosure and consent are not permitted.³

Section 206(3) and Rule 206(3)-2 – Agency Cross Trades When Acting as a Broker

Section 206(3) also prohibits an adviser, directly or indirectly, acting as broker for a person other than the advisory client, from knowingly effecting any sale or purchase of any security for the account of that client (“agency cross transactions”), without disclosing to that client in writing

* The views expressed herein are those of the staff of OCIE. This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the “SEC” or the “Commission”). The Commission has expressed no view on the contents of this Risk Alert. This Risk Alert has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by OCIE staff and is not legal advice.

¹ This Risk Alert does not discuss all of the requirements of Section 206(3) and Rule 206(3)-2 thereunder, nor does it provide an exhaustive list of compliance considerations concerning these provisions.

² This Risk Alert discusses certain issues identified in select deficiency letters from adviser exams completed during the past three years. This Risk Alert does not discuss all types of deficiencies or weaknesses related to Section 206(3) and Rule 206(3)-2 that have been identified by staff.

³ [*Commission Interpretation of Section 206\(3\) of the Investment Advisers Act of 1940*](#), Investment Advisers Act Rel. No. 1732 (July 17, 1998), 63 FR 39505 at 39507 (July 23, 1998) (“[A]n adviser may comply with Section 206(3) either by obtaining client consent prior to execution of a principal or agency transaction, or after execution but prior to settlement of the transaction.”).

before the completion of the sale or purchase the capacity in which the adviser is acting and obtaining the consent of the client to the sale or purchase. However, Advisers Act Rule 206(3)-2 permits certain agency cross transactions without requiring the adviser to provide transaction-by-transaction disclosure and consent if, among other things: (1) the client has executed a written consent prospectively authorizing agency cross trades after receiving full written disclosure of the conflicts involved and other information described in the rule; (2) the adviser provides a written confirmation to the client at or before the completion of each transaction providing, among other things, the source and amount of any remuneration it received; (3) the adviser provides a written disclosure statement to the client, at least annually, with a summary of all agency cross transactions during the period; and (4) the written disclosure documents and confirmations required by the rule conspicuously disclose that consent may be revoked at any time.⁴

Compliance with the disclosure and consent provisions of Section 206(3) alone may not satisfy an adviser's fiduciary obligations with respect to a principal or agency cross trade. To ensure that a client's consent to a principal trade or agency cross transaction is informed, the Commission has stated that Section 206(3) should be read together with Advisers Act Sections 206(1) and (2) to require the adviser to disclose facts necessary to alert the client to the adviser's potential conflicts of interest in a principal trade or agency cross transaction.⁵

II. Common Investment Adviser Compliance Issues Related to Principal and Agency Cross Trading

Below are examples of the most common deficiencies or weaknesses identified by OCIE staff in connection with Section 206(3) and Rule 206(3)-2.

A. *Section 206(3) requirements not followed.* OCIE staff observed advisers that did not appear to follow the specific requirements of Section 206(3). For example, OCIE staff observed:

- Advisers that, acting as principal for their own accounts, had purchased securities from, and sold securities to, individual clients without recognizing that such principal trades were subject to Section 206(3). Thus, these advisers did not make the required written disclosures to the clients or obtain the required client consents.
- Advisers that had recognized that they engaged in principal trades with a client, but did not meet all of the requirements of Section 206(3), such as:

⁴ Advisers and their broker-dealer affiliates should consider that Section 206(3) may apply to certain situations involving advisers that cause a client to enter into a principal or agency transaction that is effected by a broker-dealer that controls, is controlled by, or is under common control with, such adviser. *See id.* at 39505 n.3.

⁵ *See id.* at 39506; *see also* [Commission Interpretation Regarding Standard of Conduct for Investment Advisers](#), Investment Advisers Act Rel. No. 5248 at 21-23 (June 5, 2019) (“The duty of loyalty requires that an adviser not subordinate its clients’ interests to its own... To meet its duty of loyalty, an adviser must make full and fair disclosure to its clients of all material facts relating to the advisory relationship... [and] must eliminate or at least expose through full and fair disclosure all conflicts of interest which might incline an investment adviser—consciously or unconsciously—to render advice which was not disinterested”). An investment adviser also has a duty to seek best execution of a client’s transactions where the adviser has the responsibility to select broker-dealers to execute client trades (typically in the case of discretionary accounts). *See id.* at 19.

- Failing to obtain appropriate prior client consent for each principal trade.
 - Failing to provide sufficient disclosure regarding the potential conflicts of interest and terms of the transaction.⁶
 - Advisers that had obtained client consent to a principal trade *after* the completion of the transaction.
- B. *Principal trade issues related to pooled investment vehicles.* OCIE staff observed advisers that engaged in certain transactions involving pooled investment vehicle clients where such advisers did not appear to follow the requirements of Section 206(3). For example, OCIE staff observed:
- Advisers that effected trades between advisory clients and an affiliated pooled investment vehicle, but failed to recognize that the advisers' significant ownership⁷ interests in the pooled investment vehicle would cause the transaction to be subject to Section 206(3).⁸
 - Advisers that effected principal trades between themselves and pooled investment vehicle clients, but did not obtain effective consent from the pooled investment vehicle prior to completing the transactions.⁹
- C. *Agency cross transactions.* OCIE staff observed advisers' practices that gave rise to compliance issues in connection with agency cross transactions. For example, OCIE staff observed:

⁶ See [Commission Interpretation of Section 206\(3\) of the Investment Advisers Act of 1940](#), Investment Advisers Act Rel. No. 1732 (July 17, 1998), 63 FR 39505 at 39506 (July 23, 1998) ("Section 206(3) expressly requires that a client be given written disclosure of the capacity in which the adviser is acting, and that the adviser obtain its client's consent to a Section 206(3) transaction. The protection provided to advisory clients by the consent requirement of Section 206(3) would be weakened, however, without sufficient disclosure of the potential conflicts of interest and the terms of a transaction. In our view, to ensure that a client's consent to a Section 206(3) transaction is informed, Section 206(3) should be read together with Sections 206(1) and (2) to require the adviser to disclose facts necessary to alert the client to the adviser's potential conflicts of interest in a principal or agency transaction").

⁷ The Commission has entered into settlement agreements when the adviser effected transactions between their advisory clients and accounts in which the principals of the advisers held significant ownership interests. See [SEC v. Beacon Hill Asset Management, LLC](#), Litigation Rel. No. 18950 (Oct. 28, 2004) (settled matter); and [In the Matter of Gintel Asset Management](#), Investment Advisers Act Rel. No. 2079 (Nov. 8, 2002) (settled order).

⁸ Staff in the Division of Investment Management ("IM Staff") has stated its view that Section 206(3) does not apply to a transaction between a client account and a pooled investment vehicle of which the investment adviser and/or its controlling persons, in the aggregate, own 25% or less. See [Gardner Russo & Gardner](#), IM Staff No-Action Letter (June 7, 2006).

⁹ The Commission has entered into settlement agreements where an adviser to a pooled investment vehicle failed to obtain effective consent to principal trades because the review committee established by the adviser to approve the pricing of the trades in an attempt to satisfy the requirements of Section 206(3) was itself conflicted. See [Paradigm Capital Mgmt., Inc.](#), Advisers Act Rel. No. 3857 (June 16, 2014) (settled order).

- Advisers that disclosed to clients that they would not engage in agency cross transactions, but in fact engaged in numerous agency cross transactions in reliance on Rule 206(3)-2.
- Advisers that effected numerous agency cross transactions and purported to rely on Rule 206(3)-2, but could not produce any documentation that they had complied with the written consent, confirmation, or disclosure requirements of the rule.

D. *Policies and procedures related to Section 206(3)*. OCIE staff observed advisers that did not have policies and procedures relating to Section 206(3) even though the advisers engaged in principal trades and agency cross transactions.¹⁰ OCIE staff also observed advisers that established—but failed to follow—policies and procedures regarding principal trades and agency cross transactions.

III. Conclusion

In response to the issues identified in the deficiency letters, many of the advisers modified their written policies, procedures and practices to address the issues identified by OCIE staff. OCIE encourages advisers to review their written policies and procedures and the implementation of those policies and procedures to ensure that they are compliant with the principal trading and agency cross transaction provisions of the Advisers Act and the rules thereunder.

This Risk Alert is intended to highlight for firms risks and issues that OCIE staff has identified. In addition, this Risk Alert describes risks that firms may consider to (i) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (ii) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance, and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.

¹⁰ See Advisers Act Rule 206(4)-7(a) (requiring advisers to adopt and implement written policies and procedures reasonably designed to prevent violation of the Act and the rules that the Commission has adopted under the Act).

UNITED STATES¹
SECURITIES AND EXCHANGE COMMISSION

FORM CRS

OMB APPROVAL

OMB Number: 3235-0766
Expires: [Date]
Estimated average burden
hours per response: [xx.xx]

Sections 3, 10, 15, 15(c)(6), 15(l), 17, 23, and 36 of the Securities Exchange Act of 1934 (“Exchange Act”) and section 913(f) of Title IX of the Dodd-Frank Act authorize the Commission to require the collection of the information on Form CRS from brokers and dealers. *See* 15 U.S.C. 78c, 78j, 78o, 78o(c)(6), 78o(l), 78q, 78w and 78mm. Filing Form CRS is mandatory for every broker or dealer registered with the Commission pursuant to section 15 of the Exchange Act that offers services to a retail investor. *See* 17 CFR 240.17a-14. Intentional misstatements or omissions constitute federal criminal violations (*see* 18 U.S.C. 1001 and 15 U.S.C. 78ff(a)). The Commission may use the information provided in Form CRS to manage its regulatory and examination programs. Form CRS is made publically available.

An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid control number. Any member of the public may direct to the Commission any comments concerning the accuracy of this burden estimate and any suggestions for reducing this burden. This collection of information has been reviewed by the Office of Management and Budget in accordance with the requirements of 44 U.S.C. 3507.

The information contained in the form is part of a system of records subject to the Privacy Act of 1974, as amended. The information may be disclosed as outlined above and in the routine uses listed in the applicable system of records notice, SEC-70, SEC’s Division of Trading and Markets Records, published in the Federal Register at 83 FR 6892 (February 15, 2018).

SEC 2942 (06-19)

¹ This cover page will be included for Form CRS (17 CFR 249.640) only.

[Form ADV, Part 3: Instructions to Form CRS]²

General Instructions

Under rule 17a-14 under the Securities Exchange Act of 1934 and rule 204-5 under the Investment Advisers Act of 1940, broker-dealers registered under section 15 of the Exchange Act and investment advisers registered under section 203 of the Advisers Act are required to deliver to *retail investors* a *relationship summary* disclosing certain information about the firm.³ Read all the General Instructions as well as the particular item requirements before preparing or updating the *relationship summary*.

If you do not have any *retail investors* to whom you must deliver a *relationship summary*, you are not required to prepare or file one. See also Advisers Act rule 204-5; Exchange Act rule 17a-14(a).

1. Format.

- A. The *relationship summary* must include the required items enumerated below. The items require you to provide specific information.
- B. You must respond to each item and must provide responses in the same order as the items appear in these instructions. You may not include disclosure in the *relationship summary* other than disclosure that is required or permitted by these Instructions and the applicable item.
- C. You must make a copy of the *relationship summary* available upon request without charge. In paper format, the *relationship summary* for broker-dealers and investment advisers must not exceed two pages. For *dual registrants* that include their brokerage services and investment advisory services in one *relationship summary*, it must not exceed four pages in paper format. *Dual registrants* and *affiliates* that prepare separate *relationship summaries* are limited to two pages for each *relationship summary*. See General Instruction 5. You must use reasonable paper size, font size, and margins. If delivered electronically, the *relationship summary* must not exceed the equivalent of two pages or four pages in paper format, as applicable.

2. Plain English; Fair Disclosure.

- A. The items of the *relationship summary* are designed to promote effective communication between you and *retail investors*. Write your *relationship summary* in plain English, taking into consideration *retail investors'* level of

² The bracketed text will be included for Form ADV, Part 3 (17 CFR 279.1) only.

³ Terms that are italicized in these instructions are defined in General Instruction 11.

financial experience. You should include white space and implement other design features to make the *relationship summary* easy to read. The *relationship summary* should be concise and direct. Specifically: (i) use short sentences and paragraphs; (ii) use definite, concrete, everyday words; (iii) use active voice; (iv) avoid legal jargon or highly technical business terms unless you clearly explain them; and (v) avoid multiple negatives. You must write your response to each item as if you are speaking to the *retail investor*, using “you,” “us,” “our firm,” etc.

Note: The SEC’s Office of Investor Education and Advocacy has published A Plain English Handbook. You may find the handbook helpful in writing your *relationship summary*. For a copy of this handbook, visit the SEC’s website at www.sec.gov/news/extra/handbook.htm.

- B. All information in your *relationship summary* must be true and may not omit any material facts necessary in order to make the disclosures required by these Instructions and the applicable Item, in light of the circumstances under which they were made, not misleading. If a required disclosure or conversation starter is inapplicable to your business or specific wording required by these Instructions is inaccurate, you may omit or modify that disclosure or conversation starter.
- C. Responses must be factual and provide balanced descriptions to help *retail investors* evaluate your services. For example, you may not include exaggerated or unsubstantiated claims, vague and imprecise “boilerplate” explanations, or disproportionate emphasis on possible investments or activities that are not offered to *retail investors*.
- D. Broker-dealers and investment advisers have disclosure and reporting obligations under state and federal laws, including, but not limited to, obligations under the Exchange Act, the Advisers Act, and the respective rules thereunder. Broker-dealers are also subject to disclosure obligations under the rules of self-regulatory organizations. Delivery of the *relationship summary* will not necessarily satisfy the additional requirements that you have under the federal securities laws and regulations or other laws or regulations.

3. Electronic And Graphical Formats.

- A. You are encouraged to use charts, graphs, tables, and other graphics or text features in order to respond to the required disclosures. You are also encouraged to use text features, text colors, and graphical cues, such as dual-column charts, to compare services, account characteristics, investments, fees, and conflicts of interest. For a *relationship summary* that is posted on your website or otherwise provided electronically, we encourage online tools that populate information in comparison boxes based on investor selections. You also may include: (i) a means of facilitating access to video or audio messages, or other forms of information (whether by hyperlink, website address, Quick Response Code (“QR code”), or other equivalent methods or technologies); (ii) mouse-over windows;

(iii) pop-up boxes; (iv) chat functionality; (v) fee calculators; or (vi) other forms of electronic media, communications, or tools designed to enhance a *retail investor's* understanding of the material in the *relationship summary*.

- B. In a *relationship summary* that is posted on your website or otherwise provided electronically, you must provide a means of facilitating access to any information that is referenced in the *relationship summary* if the information is available online, including, for example, hyperlinks to fee schedules, conflicts disclosures, the firm's narrative brochure required by Part 2A of Form ADV, or other regulatory disclosures. In a *relationship summary* that is delivered in paper format, you may include URL addresses, QR codes, or other means of facilitating access to such information.
- C. Explanatory or supplemental information included in the *relationship summary* pursuant to General Instructions 3.A. or 3.B.: (i) must be responsive to and meet the requirements in these instructions for the particular Item in which the information is placed; and (ii) may not, because of the nature, quantity, or manner of presentation, obscure or impede understanding of the information that must be included. When using interactive graphics or tools, you may include instructions on their use and interpretation.

4. **Formatting For Conversation Starters, Additional Information, and Standard of Conduct.**

- A. For the "conversation starters" required by Items 2, 3, 4, and 5 below, you must use text features to make the conversation starters more noticeable and prominent in relation to other discussion text, for example, by: using larger or different font, a text box around the heading or questions; bolded, italicized or underlined text; or lines to offset the questions from the other sections.
- B. Investment advisers that provide only automated investment advisory services or broker-dealers that provide services only online without a particular individual with whom a *retail investor* can discuss these conversation starters must include a section or page on their website that answers each of the questions and must provide in the *relationship summary* a means of facilitating access to that section or page. If you provide automated investment advisory or brokerage services but also make a financial professional available to discuss your services with a *retail investor*, a financial professional must be available to discuss these conversation starters with the *retail investor*.
- C. For references to additional information regarding services, fees, and conflicts of interest required by Items 2.C., 3.A.(iii), and 3.B.(iv) below, you must use text features to make this information more noticeable and prominent in relation to other discussion text, for example, by: using larger or different font, a text box around the heading or questions, bolded, italicized or underlined text, or lines to offset the information from the other sections. A *relationship summary* provided

electronically must include a hyperlink, QR code, or other means of facilitating access that leads directly to the relevant additional information.

5. Dual Registrants, Affiliates, and Additional Services.

- A. If you are a *dual registrant*, you are encouraged to prepare a single *relationship summary* discussing both your brokerage and investment advisory services. Alternatively, you may prepare two separate *relationship summaries* for brokerage services and investment advisory services. Whether you prepare a single *relationship summary* or two, you must present the brokerage and investment advisory information with equal prominence and in a manner that clearly distinguishes and facilitates comparison of the two types of services. If you prepare two separate *relationship summaries*, you must reference and provide a means of facilitating access to the other, and you must deliver to each *retail investor* both *relationship summaries* with equal prominence and at the same time, without regard to whether the particular *retail investor* qualifies for those retail services or accounts.
- B. If you are a broker-dealer or investment adviser and your *affiliate* also provides brokerage or investment advisory services to *retail investors*, you may prepare a single *relationship summary* discussing the services you and your *affiliate* provide. Alternatively, you may prepare separate *relationship summaries* for your services and your *affiliate's* services.
 - (i) Whether you prepare a single *relationship summary* or separate *relationship summaries*, you must design them in a manner that presents the brokerage and investment advisory information with equal prominence and clearly distinguishes and facilitates comparison of the two types of services.
 - (ii) If you prepare separate *relationship summaries*:
 - a. If a *dually licensed financial professional* provides brokerage and investment advisory services on behalf of you and your *affiliate*, you must deliver to each *retail investor* both your and your *affiliate's relationship summaries* with equal prominence and at the same time, without regard to whether the particular *retail investor* qualifies for those retail services or accounts. Each of the *relationship summaries* must reference and provide a means of facilitating access to the other.
 - b. If General Instruction 5.B.(ii)(a) does not apply, you may choose whether or not to reference and provide a means of facilitating access to your *affiliate's relationship summary* and whether or not to deliver your and your *affiliate's relationship summaries* to each *retail investor* with equal prominence and at the same time.

- C. You may acknowledge other financial services that you provide in addition to your services as a broker-dealer or investment adviser registered with the SEC, such as insurance, banking, or retirement services, or investment advice pursuant to state registration or licensing. You may include references and means of facilitating access to additional information about those services. Information not pertaining to brokerage or investment advisory services may not, because of the nature, quantity, or manner of presentation, obscure or impede understanding of the information that must be included. See also General Instruction 3.C.

6. Preserving Records.

- A. You must maintain records in accordance with Advisers Act rule 204-2(a)(14)(i) and/or Exchange Act rule 17a-4(e)(10), as applicable.

7. Initial Filing and Delivery; Transition Provisions.

A. Initial filing.

- (i) If you are an investment adviser and are required to deliver a *relationship summary* to a *retail investor*, you must file Form ADV, Part 3 (Form CRS) electronically with the Investment Adviser Registration Depository (IARD). If you are a registered broker-dealer and are required to deliver a *relationship summary* to a *retail investor*, you must file Form CRS electronically through the Central Registration Depository (“Web CRD®”) operated by the Financial Industry Regulatory Authority, Inc. (FINRA). If you are a *dual registrant* and are required to deliver a *relationship summary* to one or more *retail investor* clients or customers of both your investment advisory and brokerage businesses, you must file using IARD and Web CRD®. You must file Form CRS using a text-searchable format with machine-readable headings.
- (ii) Information for investment advisers on how to file with IARD is available on the SEC’s website at www.sec.gov/iard. Information for broker-dealers on how to file through Web CRD® is available on FINRA’s website at <http://www.finra.org/industry/web-crd/web-crd-system-links>.

B. Initial delivery.

- (i) *Investment Advisers:* If you are an investment adviser, you must deliver a *relationship summary* to each *retail investor* before or at the time you enter into an investment advisory contract with the *retail investor*. You must deliver the *relationship summary* even if your agreement with the *retail investor* is oral. See Advisers Act rule 204-5(b)(1).
- (ii) *Broker-Dealers:* If you are a broker-dealer, you must deliver a *relationship summary* to each *retail investor*, before or at the earliest of:
 - (i) a recommendation of an account type, a securities transaction, or an investment strategy involving securities;
 - (ii) placing an order for the *retail*

investor; or (iii) the opening of a brokerage account for the *retail investor*. See Exchange Act rule 17a-14(c)(1).

- (iii) *Dual Registrants*: A dual registrant must deliver the *relationship summary* at the earlier of the timing requirements in General Instruction 7.B.(i) or (ii).

C. Transition provisions for initial filing and delivery after the effective date of the new Form CRS requirements.

(i) *Filings for Investment Advisers*

- a. If you are already registered or have an application for registration pending with the SEC as an investment adviser before June 30, 2020 you must electronically file, in accordance with Instruction 7.A. above, your initial *relationship summary* beginning on May 1, 2020 and by no later than June 30, 2020 either as: (1) an other-than-annual amendment or (2) part of your initial application or *annual updating amendment*. See Advisers Act rules 203-1 and 204-1.
- b. If you file an application for registration with the SEC as an investment adviser on or after June 30, 2020, the Commission will not accept any initial application that does not include a *relationship summary*. See Advisers Act rule 203-1.

(ii) *Filings for Broker-Dealers*

- a. If you are already registered with the SEC as a broker-dealer before June 30, 2020, you must electronically file, in accordance with Instruction 7.A. above, your initial *relationship summary* beginning on May 1, 2020 and by no later than June 30, 2020. See Exchange Act rule 17a-14.
- b. If you file an application for registration or have an application pending with the SEC as a broker-dealer on or after June 30, 2020, you must file your *relationship summary* by no later than the date that your registration becomes effective. See Exchange Act rule 17a-14.

- (iii) *Delivery to New and Prospective Clients and Customers*: As of the date by which you are first required to electronically file your *relationship summary* with the SEC, you must begin to deliver your *relationship summary* to new and prospective clients and customers who are *retail investors* as required by Instruction 7.B. See Advisers Act rule 204-5 and Exchange Act rule 17a-14.

- (iv) *Delivery to Existing Clients and Customers*: Within 30 days after the date by which you are first required to electronically file your *relationship*

summary with the SEC, you must deliver your *relationship summary* to each of your existing clients and customers who are *retail investors*. See Advisers Act rule 204-5 and Exchange Act rule 17a-14.

8. Updating the *Relationship Summary* and Filing Amendments.

- A. You must update your *relationship summary* and file it in accordance with Instruction 7.A. above within 30 days whenever any information in the *relationship summary* becomes materially inaccurate. The filing must include an exhibit highlighting changes required by Instruction 8.C. below.
- B. You must communicate any changes in the updated *relationship summary* to *retail investors* who are existing clients or customers within 60 days after the updates are required to be made and without charge. You can make the communication by delivering the amended *relationship summary* or by communicating the information through another disclosure that is delivered to the *retail investor*.
- C. Each amended *relationship summary* that is delivered to a *retail investor* who is an existing client or customer must highlight the most recent changes by, for example, marking the revised text or including a summary of material changes. The additional disclosure showing revised text or summarizing the material changes must be attached as an exhibit to the unmarked amended *relationship summary*.

9. Additional Delivery Requirements to Existing Clients and Customers.

- A. You must deliver the most recent *relationship summary* to a *retail investor* who is an existing client or customer before or at the time you: (i) open a new account that is different from the *retail investor's* existing account(s); (ii) recommend that the *retail investor* roll over assets from a retirement account into a new or existing account or investment; or (iii) recommend or provide a new brokerage or investment advisory service or investment that does not necessarily involve the opening of a new account and would not be held in an existing account, for example, the first-time purchase of a direct-sold mutual fund or insurance product that is a security through a “check and application” process, *i.e.*, not held directly within an account.
- B. You also must deliver the *relationship summary* to a *retail investor* within 30 days upon the *retail investor's* request.

10. Electronic Posting and Manner of Delivery.

- A. You must post the current version of the *relationship summary* prominently on your public website, if you have one, in a location and format that is easily accessible for *retail investors*.

- B. You may deliver the *relationship summary* electronically, including updates, consistent with SEC guidance regarding electronic delivery, in particular Use of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery of Information, which you can find at www.sec.gov/rules/concept/33-7288.txt. You may deliver the *relationship summary* to new or prospective clients or customers in a manner that is consistent with how the *retail investor* requested information about you or your financial professional consistent with SEC guidance, in particular Form CRS Relationship Summary; Amendments to Form ADV, which you can find at <https://www.sec.gov/rules/final/2019/34-86032.pdf>.
- C. If the *relationship summary* is delivered electronically, it must be presented prominently in the electronic medium, for example, as a direct link or in the body of an email or message, and must be easily accessible for *retail investors*.
- D. If the *relationship summary* is delivered in paper format as part of a package of documents, you must ensure that the *relationship summary* is the first among any documents that are delivered at that time.

11. **Definitions.**

For purposes of Form CRS and these Instructions, the following terms have the meanings ascribed to them below:

- A. **Affiliate:** Any persons directly or indirectly controlling or controlled by you or under common control with you.
- B. **Dually licensed financial professional:** A natural person who is both an associated person of a broker-dealer registered under section 15 of the Exchange Act, as defined in section 3(a)(18) of the Exchange Act, and a supervised person of an investment adviser registered under section 203 of the Advisers Act, as defined in section 202(a)(25) of the Advisers Act.
- C. **Dual registrant:** A firm that is dually registered as a broker-dealer under section 15 of the Exchange Act and an investment adviser under section 203 of the Advisers Act and offers services to *retail investors* as both a broker-dealer and an investment adviser. For example, if you are dually registered and offer investment advisory services to *retail investors*, but offer brokerage services only to institutional investors, you are not a *dual registrant* for purposes of Form CRS and these Instructions.
- D. **Relationship summary:** A written disclosure statement prepared in accordance with these Instructions that you must provide to *retail investors*. See Advisers Act rule 204-5; Exchange Act rule 17a-14; Form CRS.
- E. **Retail investor:** A natural person, or the legal representative of such natural person, who seeks to receive or receives services primarily for personal, family or household purposes.

Item Instructions

Item 1. Introduction

Include the date prominently at the beginning of the *relationship summary* (e.g., in the header or footer of the first page or in a similar location for a *relationship summary* provided electronically). Briefly discuss the following information in an introduction:

- A. State your name and whether you are registered with the Securities and Exchange Commission as a broker-dealer, investment adviser, or both. Also indicate that brokerage and investment advisory services and fees differ and that it is important for the *retail investor* to understand the differences. You may also include a reference to FINRA or Securities Investor Protection Corporation membership in a manner consistent with other rules or regulations (e.g., FINRA rule 2210).
- B. State that free and simple tools are available to research firms and financial professionals at Investor.gov/CRS, which also provides educational materials about broker-dealers, investment advisers, and investing.

Item 2. Relationships and Services

- A. Use the heading: “What investment services and advice can you provide me?”
- B. **Description of Services:** State that you offer brokerage services, investment advisory services, or both, to *retail investors*, and summarize the principal services, accounts, or investments you make available to *retail investors*, and any material limitations on such services. For broker-dealers, state the particular types of principal brokerage services you offer to *retail investors*, including buying and selling securities, and whether or not you offer recommendations to *retail investors*. For investment advisers, state the particular types of principal investment advisory services you offer to *retail investors*, including, for example, financial planning and wrap fee programs.

In your description you must address the following:

- (i) *Monitoring:* Explain whether or not you monitor *retail investors’* investments, including the frequency and any material limitations. If so, indicate whether or not the services described in response to this Item 2.B.(i) are offered as part of your standard services.
- (ii) *Investment Authority:* For investment advisers that accept discretionary authority, describe those services and any material limitations on that authority. Any such summary must include the specific circumstances that would trigger this authority and any material limitations on that authority (e.g., length of time). For investment advisers that offer non-discretionary services and broker-dealers, explain that the *retail investor* makes the ultimate decision regarding the purchase or sale of investments.

Broker-dealers may, but are not required to state whether you accept limited discretionary authority.

Note: If you are a broker-dealer offering recommendations, you should consider the applicability of the Investment Advisers Act of 1940, consistent with SEC guidance.

- (iii) *Limited Investment Offerings*: Explain whether or not you make available or offer advice only with respect to proprietary products, or a limited menu of products or types of investments, and if so, describe these limitations.
- (iv) *Account Minimums and Other Requirements*: Explain whether or not you have any requirements for *retail investors* to open or maintain an account or establish a relationship, such as minimum account size or investment amount.

C. **Additional Information:** Include specific references to more detailed information about your services that, at a minimum, include the same or equivalent information to that required by the Form ADV, Part 2A brochure (Items 4 and 7 of Part 2A or Items 4.A. and 5 of Part 2A Appendix 1) and Regulation Best Interest, as applicable. If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, to the extent you prepare more detailed information about your services, you must include specific references to such information. You may include hyperlinks, mouse-over windows, or other means of facilitating access to this additional information and to any additional examples or explanations of such services.

D. **Conversation Starters:** Include the following additional questions for a *retail investor* to ask a financial professional and start a conversation about relationships and services:

- (i) If you are a broker-dealer and not a *dual registrant*, include: “Given my financial situation, should I choose a brokerage service? Why or why not?”
- (ii) If you are an investment adviser and not a *dual registrant*, include: “Given my financial situation, should I choose an investment advisory service? Why or why not?”
- (iii) If you are a *dual registrant*, include: “Given my financial situation, should I choose an investment advisory service? Should I choose a brokerage service? Should I choose both types of services? Why or why not?”
- (iv) “How will you choose investments to recommend to me?”
- (v) “What is your relevant experience, including your licenses, education and other qualifications? What do these qualifications mean?”

Item 3. Fees, Costs, Conflicts, and Standard of Conduct

A. Use the heading: “What fees will I pay?”

- (i) *Description of Principal Fees and Costs:* Summarize the principal fees and costs that *retail investors* will incur for your brokerage or investment advisory services, including how frequently they are assessed and the conflicts of interest they create.
 - a. Broker-dealers must describe their transaction-based fees. With respect to addressing conflicts of interest, a broker-dealer could, for example, include a statement that a *retail investor* would be charged more when there are more trades in his or her account, and that the firm may therefore have an incentive to encourage a *retail investor* to trade often.
 - b. Investment advisers must describe their ongoing asset-based fees, fixed fees, wrap fee program fees, or other direct fee arrangement. The principal fees for investment advisory services should align with the type of fee(s) that you report in response to Form ADV Part 1A, Item 5.E.
 - (1) Include information about each type of fee you report in Form ADV that is responsive to this Item 3.A. Investment advisers with wrap fee program fees are encouraged to explain that asset-based fees associated with the wrap fee program will include most transaction costs and fees to a broker-dealer or bank that has custody of these assets, and therefore are higher than a typical asset-based advisory fee.
 - (2) With respect to addressing conflicts of interest, an investment adviser that charges an asset-based fee could, for example, include a statement that the more assets there are in a *retail investor’s* advisory account, the more a *retail investor* will pay in fees, and the firm may therefore have an incentive to encourage the *retail investor* to increase the assets in his or her account.
- Note:** If you receive compensation in connection with the purchase or sale of securities, you should carefully consider the applicability of the broker-dealer registration requirements of the Securities Exchange Act of 1934 and any applicable state securities statutes.
- (ii) *Description of Other Fees and Costs:* Describe other fees and costs related to your brokerage or investment advisory services and investments in addition to the firm’s principal fees and costs disclosed in Item 3.A.(i) that the *retail investor* will pay directly or indirectly. List examples of the

categories of the most common fees and costs applicable to your *retail investors* (e.g., custodian fees, account maintenance fees, fees related to mutual funds and variable annuities, and other transactional fees and product-level fees).

- (iii) *Additional Information*: State “You will pay fees and costs whether you make or lose money on your investments. Fees and costs will reduce any amount of money you make on your investments over time. Please make sure you understand what fees and costs you are paying.” You must include specific references to more detailed information about your fees and costs that, at a minimum, include the same or equivalent information to that required by the Form ADV, Part 2A brochure (specifically Items 5.A., B., C., and D.) and Regulation Best Interest, as applicable. If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, to the extent you prepare more detailed information about your fees and costs, you must include specific references to such information. You may include hyperlinks, mouse-over windows, or other means of facilitating access to this additional information and to any additional examples or explanations of such fees and costs included in response to Item 3.A.(i) or (ii).
- (iv) *Conversation Starter*: Include the following question for a *retail investor* to ask a financial professional and start a conversation about the impact of fees and costs on investments: “Help me understand how these fees and costs might affect my investments. If I give you \$10,000 to invest, how much will go to fees and costs, and how much will be invested for me?”

B. If you are a broker-dealer, use the heading: “What are your legal obligations to me when providing recommendations? How else does your firm make money and what conflicts of interest do you have?” If you are an investment adviser, use the heading: “What are your legal obligations to me when acting as my investment adviser? How else does your firm make money and what conflicts of interest do you have?” If you are a *dual registrant* that prepares a single *relationship summary*, use the heading: “What are your legal obligations to me when providing recommendations as my broker-dealer or when acting as my investment adviser? How else does your firm make money and what conflicts of interest do you have?”

- (i) *Standard of Conduct*.
 - a. If you are a broker-dealer that provides recommendations subject to Regulation Best Interest, include (emphasis required): “*When we provide you with a recommendation, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because*

they can affect the recommendations we provide you. Here are some examples to help you understand what this means.” If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, include (emphasis required): “We *do not* provide recommendations. The way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the services we provide you. Here are some examples to help you understand what this means.”

- b. If you are an investment adviser, include (emphasis required): “*When we act as your investment adviser*, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the investment advice we provide you. Here are some examples to help you understand what this means.”
- c. If you are a *dual registrant* that prepares a single *relationship summary* and you provide recommendations subject to Regulation Best Interest as a broker-dealer, include (emphasis required): “*When we provide you with a recommendation as your broker-dealer or act as your investment adviser*, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the recommendations and investment advice we provide you. Here are some examples to help you understand what this means.” If you are a *dual registrant* that prepares a single *relationship summary* and you do not provide recommendations subject to Regulation Best Interest as a broker-dealer, include (emphasis required): “We *do not* provide recommendations as your broker-dealer. *When we act as your investment adviser*, we have to act in your best interest and not put our interests ahead of yours. At the same time, the way we make money creates some conflicts with your interest. You should understand and ask us about these conflicts because they can affect the services and investment advice we provide you. Here are some examples to help you understand what this means.” If you are a *dual registrant* that prepares two separate *relationship summaries*, follow the instructions for broker-dealers and investment advisers in Items 3.B., 3.B.(i).a., and 3.B.(i).b.

- (ii) *Examples of Ways You Make Money and Conflicts of Interest:* If applicable to you, summarize the following other ways in which you and your *affiliates* make money from brokerage or investment advisory

services and investments you provide to *retail investors*. If none of these conflicts applies to you, summarize at least one other material conflict of interest that affects *retail investors*. Explain the incentives created by each of these examples.

- a. Proprietary Products: Investments that are issued, sponsored, or managed by you or your *affiliates*.
- b. Third-Party Payments: Compensation you receive from third parties when you recommend or sell certain investments.
- c. Revenue Sharing: Investments where the manager or sponsor of those investments or another third party (such as an intermediary) shares with you revenue it earns on those investments.
- d. Principal Trading: Investments you buy from a *retail investor*, and/or investments you sell to a *retail investor*, for or from your own accounts, respectively.

(iii) *Conversation Starter*: Include the following question for a *retail investor* to ask a financial professional and start a conversation about conflicts of interest: “How might your conflicts of interest affect me, and how will you address them?”

(iv) *Additional Information*: You must include specific references to more detailed information about your conflicts of interest that, at a minimum, include the same or equivalent information to that required by the Form ADV, Part 2A brochure and Regulation Best Interest, as applicable. If you are a broker-dealer that does not provide recommendations subject to Regulation Best Interest, to the extent you prepare more detailed information about your conflicts, you must include specific references to such information. You may include hyperlinks, mouse-over windows, or other means of facilitating access to this additional information and to any additional examples or explanations of such conflicts of interest.

C. Use the heading: “How do your financial professionals make money?”

(i) *Description of How Financial Professionals Make Money*: Summarize how your financial professionals are compensated, including cash and non-cash compensation, and the conflicts of interest those payments create.

(ii) *Required Topics in the Description*: Include, to the extent applicable, whether your financial professionals are compensated based on factors such as: the amount of client assets they service; the time and complexity required to meet a client’s needs; the product sold (*i.e.*, differential compensation); product sales commissions; or revenue the firm earns from the financial professional’s advisory services or recommendations.

Item 4. Disciplinary History

- A. Use the heading: “Do you or your financial professionals have legal or disciplinary history?”
- B. State “Yes” if you or any of your financial professionals currently disclose, or are required to disclose, the following information:
 - (i) Disciplinary information in your Form ADV (Item 11 of Part 1A or Item 9 of Part 2A).
 - (ii) Legal or disciplinary history in your Form BD (Items 11 A–K) (except to the extent such information is not released to BrokerCheck, pursuant to FINRA Rule 8312).
 - (iii) Disclosures for any of your financial professionals in Items 14 A–M on Form U4 (Uniform Application for Securities Industry Registration or Transfer), or in Items 7A or 7C–F of Form U5 (Uniform Termination Notice for Securities Industry Registration), or on Form U6 (Uniform Disciplinary Action Reporting Form) (except to the extent such information is not released to BrokerCheck, pursuant to FINRA Rule 8312).
- C. State “No” if neither you nor any of your financial professionals currently discloses, or is required to disclose, the information listed in Item 4.B.
- D. Regardless of your response to Item 4.B, you must:
 - (i) *Search Tool*: Direct the *retail investor* to visit Investor.gov/CRS for a free and simple search tool to research you and your financial professionals.
 - (ii) *Conversation Starter*: Include the following questions for a *retail investor* to ask a financial professional and start a conversation about the financial professional’s disciplinary history: “As a financial professional, do you have any disciplinary history? For what type of conduct?”

Item 5. Additional Information

- A. State where the *retail investor* can find additional information about your brokerage or investment advisory services and request a copy of the *relationship summary*. This information should be disclosed prominently at the end of the *relationship summary*.
- B. Include a telephone number where *retail investors* can request up-to-date information and request a copy of the *relationship summary*.

- C. **Conversation Starter:** Include the following questions for a *retail investor* to ask a financial professional and start a conversation about the contacts and complaints: “Who is my primary contact person? Is he or she a representative of an investment adviser or a broker-dealer? Who can I talk to if I have concerns about how this person is treating me?”

Form CRS Disclosure Template for Standalone Investment Advisers
Prepared by Investment Adviser Association – For Illustrative Purposes Only

[Date] [Item 1]

[Name] [1.A.]

[State registered with the Securities and Exchange Commission as an Investment Adviser.] [1.A.]

[Indicate that brokerage and investment advisory services and fees differ and that it is important for the retail investor to understand the differences.] [1.A.] [State that free and simple tools are available to research firms and financial professionals at [Investor.gov/CRS](https://investor.gov/CRS), which also provides educational materials about broker-dealers, investment advisers, and investing.] [1.B.]

What investment services and advice can you provide me? [Item 2.A.]

[State that you offer brokerage, investment advisory, or both, services to retail investors. Summarize principal services, accounts, or investments you make available to retail investors, and any material limitations on such services. State particular types of principal advisory services, including, for example, financial planning and wrap fee programs. Must address: monitoring, including frequency and material limitations (part of standard services?); describe discretionary authority, including material limitations; for non-discretionary, explain that client makes ultimate decision; describe any limited investment offerings; account minimums, size, and other requirements to open or maintain account(s).] [2.B.]

INCLUDE SPECIFIC REFERENCES TO MORE DETAILED INFORMATION ABOUT YOUR SERVICES THAT, AT A MINIMUM, INCLUDE THE SAME OR EQUIVALENT INFORMATION TO THAT REQUIRED BY THE FORM ADV, PART 2A BROCHURE (ITEMS 4 AND 7 OF PART 2A OR ITEMS 4.A. AND 5 OF PART 2A APPENDIX 1). [2.C.]

Given my financial situation, should I choose an investment advisory service? Why or why not? [2.D.]

How will you choose investments to recommend to me? [2.D.]

What is your relevant experience, including your licenses, education and other qualifications? What do these qualifications mean? [2.D.]

What fees will I pay? [Item 3]

[Summarize principal fees and costs, including how frequently assessed and related conflicts.] [3.A.(i)] [Describe ongoing asset-based fees, fixed fees, wrap fee program fees, or other direct fee arrangements.] [3.A.(i)b] [RIAs with wrap program fees explain fees associated with program include most transaction costs and fees to BD or bank that has custody of these assets, and therefore are higher than typical asset-based advisory fee.] [3.A.(i)b(1)] [In addressing conflict, may include statement that more assets in account means more fees, thus incentive to encourage client to increase assets in account.] [3.A.(i).b.(2)] [Describe other fees and costs client will pay directly or indirectly. List examples of most common categories (e.g., custodian fees, account maintenance fees, fees related to mutual funds and variable annuities, and other transactional fees and product-level fees).] [3.A.(ii)]

You will pay fees and costs whether you make or lose money on your investments. Fees and costs will reduce any amount of money you make on your investments over time. Please make sure you understand what fees and costs you are paying. [3.A.(iii)]

INCLUDE SPECIFIC REFERENCES TO MORE DETAILED INFORMATION ABOUT YOUR FEES AND COSTS THAT, AT A MINIMUM, INCLUDE THE SAME OR EQUIVALENT INFORMATION FROM FORM ADV, PART 2A BROCHURE (ITEMS 5.A., B., C., AND D.). [3.A.(iii)]

Help me understand how these fees and costs might affect my investments. If I give you \$10,000 to invest, how much will go to fees and costs, and how much will be invested for me? [3.A.(iv)]

What are your legal obligations to me when acting as my investment adviser? How else does your firm make money and what conflicts of interest do you have? [3.B.]

When we act as your investment adviser, we have to act in your best interest and not put our interest ahead of yours. At the same time, the way we make money creates some conflicts with your interests. You should understand and ask us about these conflicts because they can affect the investment advice we provide you. Here are some examples to help you understand what this means. [3.B.(i)b.]

[If applicable, summarize other ways you and your affiliates make money and related incentives. For example, proprietary investments issued, sponsored, or managed by you or affiliates; compensation received from third parties when recommending or selling certain investments; revenue sharing arrangements; principal trading. If none of these conflicts exist, summarize at least one other material conflict of interest that affects retail investors.] [3.B.(ii)]

INCLUDE SPECIFIC REFERENCES TO MORE DETAILED INFORMATION ABOUT CONFLICTS OF INTEREST, AT A MINIMUM, SAME OR EQUIVALENT TO FORM ADV, PART 2A BROCHURE. [3.B.(iv)]

How might your conflicts of interest affect me, and how will you address them? [3.B.(iii)]

How do your financial professionals make money? [3.C.]

[Summarize how FPs are compensated, including cash and non-cash compensation, and the conflicts of interest those payments create.] [3.C.(i)] [Include whether FP compensation based on factors such as: amount of client assets they service; time and complexity required to meet a client's needs; product sold (i.e., differential compensation); product sales commissions; or revenue firm earns from FP's advisory services or recommendations.] [3.C.(ii)]

Do you or your financial professionals have legal or disciplinary history? [Item 4.A.]

[State "Yes" [4.B.] or "No". [4.C.]] [Direct to [Investor.gov/CRS](https://www.investor.gov/crs) for free and simple search tool to research you and your financial professionals.] [4.D.(i)]

As a financial professional, do you have any disciplinary history? For what type of conduct? [4.D.(ii)]

[State where additional information can be obtained.] [Item 5.A.] [Include telephone number for clients to request up-to-date information and request copy of CRS.] [Item 5.B.]

Who is my primary contact person? Is he or she a representative of an investment adviser or a broker-dealer? Who can I talk to if I have concerns about how this person is treating me? [5.C.]

**Hedge Funds Luncheon Series:
Winter Regulatory Update 2020**

March 6, 2020

Recent OCIE Exam Questions (Paraphrased)

Key “Normal” Initial Requests

Claims, proceedings: Any *threatened*, pending, and settled litigation or arbitration involving Registrant or any “supervised person” (if the matter relates to the supervised person’s association with Registrant or a securities-related matter) including a description of the allegations, the status, and a brief description of any “out of court” or informal settlement. Note that “supervised person” is any partner, officer, director (or other person occupying a similar status or performing similar functions), or employee of an investment adviser, or other person who provides investment advice on behalf of the investment adviser and is subject to the supervision and control of the investment adviser (defined in Section 202(a)(25) of the Investment Advisers Act of 1940). If none, please provide a written statement to that effect.

Employees, consultants: In Excel, a list of current full-time and part-time employees, interns, *consultants, secondees*, partners, directors, officers, *strategic advisors, operating advisors, senior advisors or similar*, as applicable. Provide titles, areas of responsibility, start and departure dates (as applicable), locations(s), whether the individual has been deemed an access persons for purpose of the Registrant’s Code of Ethics and whether the individual is exempt from any of the Registrant’s other compliance policies and procedures. Note if any of the above individuals *resigned, were disciplined for compliance purposes, or terminated, along with the dates and reason for termination, discipline or resignation*. Provide any executed separation agreement.

Names of any of the Registrants' officers, employees, and/or directors who resigned, were *disciplined, and/or terminated* and information regarding the reason for their departure.

Compliance Program:

Compliance and operational policies and procedures in effect during the Examination Period for the Registrant and its affiliates. Please be sure to also include any Code of Ethics, insider trading, fair valuation, remote office monitoring, contractor oversight, and GIPS policies and procedures that are created and maintained.

Any *written interim and annual compliance reviews, internal control analyses, exception reports, and forensic or transactional tests performed*. Include *any significant findings, both positive and negative*, and any information about corrective or remedial actions taken regarding these findings.

A *current inventory of the Registrant’s compliance risks* that forms the basis for its policies and procedures. Note any changes made to the inventory during the Examination Period and the dates of the changes.

Written guidance the Registrant provided to its employees regarding the compliance program and ***documents evidencing employee compliance training*** during the Examination Period.

A list of all client or investor complaints and information about the process used for monitoring client/investor correspondence and/or complaints.

A record of any non-compliance with the Registrant's compliance policies and procedures and of any action taken as a result of such non-compliance.

List and describe any automated systems or tools used to carry out key compliance-related oversight functions and/or reporting obligations.

Additional Increasingly Common Follow-up Questions:

Compliance: Description of compliance framework (including the use of ***all third party service providers*** who assist with compliance (i.e., ***law firms and consultants***))

A copy of any compliance-related reports produced by a consultant or other third party during the Examination Period.

Alternative Data: Please provide:

1. Registrant's processes and procedures for identifying, vetting, testing, implementing, and monitoring entities or individuals that provide or make available information that is utilized in the investment decision making process pursuant to a contractual agreement (collectively "Data and Research Providers"). Data and Research Providers would include but not be limited to research consultants, expert networks, data aggregators, survey companies, entities selling data from their own business operations (sometimes called "business exhaust data"), entities that assist with the extraction, transformation and loading of data (commonly referred to as ETL), broker-dealers supplying research or data, and providers of market data, web scraped data, consumer spending data, satellite images, supply chain data, flight tracking data, geolocation data, factor analysis, political intelligence and analyst reports;
2. Data collection efforts of internal staff or affiliated entities to make available or structure data that is utilized for Registrant's investment activities; Registrant should describe any collection of data from other parts of the Registrant or their affiliate's businesses in the investment decision-making process. Registrant should also describe any collection of data by employees through direct efforts of the Registrant or their employees (e.g. web scraping, surveys, channel checking, etc.);
3. Allocation and availability of data across clients and portfolio managers;
4. Structure and use of research consultants that make portfolio recommendations;
5. Structure and use of experts and expert networks; and
6. Oversight process with respect to the potential receipt of material, non-public information.

Valuation: Please indicate any instances where there were *valuation discrepancies noted by the auditor* and brought to the attention of the Registrant. Please provide a narrative describing the situation, including but not limited to the name of the investment, and how it was resolved.

MNPI: Please describe Registrant's oversight process with respect to the potential receipt of material, non-public information.

Provide support for surveillance of trading in close proximity to one-on-one discussions with expert network consultants, private fund managers and/or corporate insiders.

NDAs: Please provide in Excel a log of any non-disclosure agreements ("NDA") entered into by the Registrant during or covered by the Examination Period (exclude NDA's entered into with employees). Include the following information: subject matter (e.g., systems vendor, potential deal, etc.), parties to the agreement (with respect to the Registrant's related persons, note the affiliation to the Registrant), effective date, expiration date, whether there are any standstill provisions and if so, any termination date of the standstill, and subject/target companies covered by any deal-related NDAs.

Trading Models: Please describe how the Compliance Department monitors the development, testing and use of trading models used by portfolio managers?

Text Messages: Please provide a list of all services, such as Confide or Snapchat, used by employees for business purposes, that automatically destroy messages sent after a given period of time.

Please inform the Staff if any electronic communications during the time periods requested were not maintained.

Investment Thesis: For the companies noted below, provide investment thesis and information explaining the rationale for the trading over the time period noted. Please also provide documents supporting analysis or other records pertaining to investment decisions.

Alternative Data: Current Legal and Compliance Issues

March 6, 2020

Presenter:

Robert Leonard

Proskauer»

Summary

- Emergence of “Alternative Data” as an industry trend.
- What is “Alternative Data?” Describe the various techniques for acquiring the data.
- What are the key legal issues/concerns raised by the use of “Alternative Data”?
- What are the key takeaways for fund managers?
- Discuss policies, procedures and practices.
- Recent news

What Is Alt Data for Hedge Funds?



What Is Alt Data for Hedge Funds?



What Is Alt Data for Hedge Funds?



What Is Alt Data for Hedge Funds?



What Is Alt Data for Hedge Funds?



What Is Alt Data for Hedge Funds?



Privacy Issues



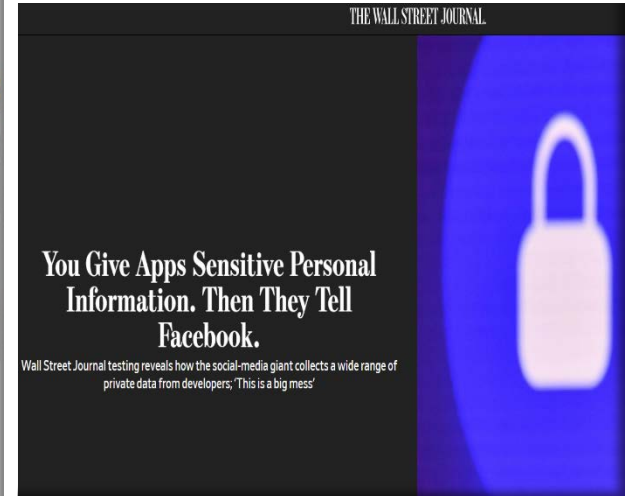
YOU ARE BEING TRACKED

How License Plate Readers Are Being Used To Record Americans' Movements



A little noticed surveillance technology, designed to track the movements of every passing driver, is fast proliferating on America's streets. Automatic license plate readers, mounted on police cars or on objects like road signs and bridges, use small, high-speed cameras to photograph thousands of plates per minute.

The information captured by the readers—including the license plate number, and the date, time, and location of every scan—is being collected and



Privacy Issues



California and Nevada Privacy Laws

- CCPA took effect on Jan. 1, 2020
- Includes the **right to opt-out** of sale of PI. Consumers will be able to direct a business that sells PI to stop selling that information.
- Businesses must create procedures to respond to such requests and include a “Do Not Sell My Info” link on their website or mobile app.
- Businesses must respond to requests from consumers to know, delete, and opt-out within specific timeframes.
- As proposed by the Attorney General’s draft regulations, businesses must treat user-enabled privacy settings that signal a consumer’s choice to opt-out as a validly submitted opt-out request.

California and Nevada Privacy Laws

- **Oct. 1, 2019**: Nevada's privacy law amendments (SB220) became effective
- Notably, includes a consumer right to opt out from the sale of personal information
 - “Sale” means “the exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons.”
 - Exemptions apply, incl.: disclosure of covered information by an operator to a person “for purposes which are consistent with the reasonable expectations of a consumer”
- “Operators” are defined as persons who own or operate websites or online services for commercial purposes that (1) collect and maintain “Covered Information” (various common items of PII) and (2) purposefully directs its activities toward Nevada or otherwise engages in activities that establish a sufficient nexus with the state of Nevada.
- Exemptions from “Operators”
 - Third parties that operate, host or manage a website and 3P service providers
 - Financial institutions subject to the Gramm-Leach-Bliley Act
 - Entities subject to HIPAA
 - Manufacturers of motor vehicles and persons who repair or service cars

Data Broker Laws

- **Jan, 2019:** Vermont law imposed annual disclosure requirements on “data brokers” if the broker has data of Vermont residents.
 - Annual disclosure must also specify what, if any, opt-out rights exist for consumers.
 - “Data broker” means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.
 - “Brokered Personal Information” means PII + “other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty”
 - “A person shall not acquire brokered personal information through fraudulent means.” 9 V.S.A. Section 2431
- **Oct. 2019:** California passed Data Broker Law
 - Law requires data brokers to register with, and provide certain information to, the Attorney General (e.g., name, address, optional explanation of data collection practices). The AG would make information provided by brokers available to the public.
 - Data broker is defined as a “business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.”
 - “Sale” and “personal information” takes definition from CCPA

Mobile Phone Issues

- **Apple Store Review Guidelines**
 - **Section 5.1.2(i):**
 - Unless otherwise permitted by law, you may not use, transmit, or share someone's personal data without first obtaining their permission. You must provide access to information about how and where the data will be used. **Data collected from apps may only be shared with third parties** to improve the app or serve advertising (in compliance with the [Apple Developer Program License Agreement](#)). Apps that share user data without user consent or otherwise complying with data privacy laws may be removed from sale and may result in your removal from the Apple Developer Program.
 - **Section 5.1.2(ii):**
 - Data collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law.
 - **Apple Developer Program License Agreement Section 3.3.9:**
 - You and Your Applications ... may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising ... You may not use analytics software in Your Application to collect and send device data to a third party.

The People of California v. The Weather Channel

- L.A. City Attorney filed an unfair competition lawsuit for allegedly failing to conspicuously disclose to users that the TWC app collects and shares users' mobile geolocation data.
- The suit alleges that the TWC app mines users' precise geolocation data after receiving permission to gather location information to provide "personalized local weather data" without also adequately disclosing that the app also packages anonymized data to 3Ps for advertising and analytics services unrelated to weather reporting.



1 MICHAEL N. FEUER, City Attorney (SBN 111529)
2 JAMES P. CLARK, Chief Deputy City Attorney (SBN 64780)
3 THOMAS H. PETERS, Chief Assistant City Attorney (SBN 163388)
4 MICHAEL J. BOSTROM, Assistant City Attorney (SBN 211778)
5 ADAM R. TEITELBAUM, Deputy City Attorney (SBN 310565)
6 OFFICE OF THE LOS ANGELES CITY ATTORNEY
200 North Spring Street, 14th Floor
Los Angeles, CA 90012-4131
Telephone: (213) 978-1865
Facsimile: (213) 978-2286
Email: adam.teitelbaum@lacity.org

7 Attorneys for Plaintiff,
8 THE PEOPLE OF THE STATE OF CALIFORNIA

9 [NO FEE – Cal. Govt. Code § 6103]
10 SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF LOS ANGELES

11 THE PEOPLE OF THE STATE OF CALIFORNIA, Case No.: _____
12 CALIFORNIA, Plaintiff,
13 v. COMPLAINT FOR INJUNCTIVE
14 TWC PRODUCT AND TECHNOLOGY, LLC, RELIEF AND CIVIL PENALTIES FOR
15 a Delaware corporation; and DOES 1-50, VIOLATIONS OF THE UNFAIR
16 inclusive, COMPETITION LAW (CALIFORNIA
BUSINESS & PROFESSIONS CODE
§§ 17200, ET SEQ.)


17 Defendants.

INTRODUCTION

1 I. Plaintiff People of the State of California ("the People"), by and through
2 Michael N. Feuer, the City Attorney of Los Angeles, bring this civil law enforcement action

The People of California v. The Weather Channel

- L.A. City Attorney filed an unfair competition lawsuit for allegedly failing to conspicuously disclose to users that the TWC app collects and shares users' mobile geolocation data.
- The suit alleges that the TWC app mines users' precise geolocation data after receiving permission to gather location information to provide "personalized local weather data" without also adequately disclosing that the app also packages anonymized data to 3Ps for advertising and analytics services unrelated to weather reporting.



Location and Your Weather

Did you know sharing your device's location and pressure sensor data helps us provide you with the most accurate weather?

As our [Privacy Policy](#) describes, when you grant permission we use and may share your device's location with trusted partners to deliver forecasts, weather alerts, and ads, and to provide and improve our Services. You can change permissions at any time. [Learn More.](#)

I Understand

MICHAEL N. FEUER, City Attorney (SBN 111529)
JAMES P. CLARK, Chief Deputy City Attorney (SBN 64780)
THOMAS H. PETERS, Chief Assistant City Attorney (SBN 163388)
MICHAEL J. BOSTROM, Assistant City Attorney (SBN 211778)
ADAM R. TEITELBAUM, Deputy City Attorney (SBN 310565)
OFFICE OF THE LOS ANGELES CITY ATTORNEY
200 North Spring Street, 14th Floor
Los Angeles, CA 90012-4131
Telephone: (213) 978-1865
Facsimile: (213) 978-2286
Email: adam.teitelbaum@lacity.org

Attorneys for Plaintiff,
THE PEOPLE OF THE STATE OF CALIFORNIA

[NO FEE – Cal. Govt. Code § 6103]

SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF LOS ANGELES

THE PEOPLE OF THE STATE OF CALIFORNIA, Case No.: _____
Plaintiff,
v.
TWC PRODUCT AND TECHNOLOGY, LLC,
a Delaware corporation; and DOES 1-50,
inclusive,
Defendants.

COMPLAINT FOR INJUNCTIVE RELIEF AND CIVIL PENALTIES FOR VIOLATIONS OF THE UNFAIR COMPETITION LAW (CALIFORNIA BUSINESS & PROFESSIONS CODE §§ 17200, ET SEQ.)

INTRODUCTION

I. Plaintiff People of the State of California ("the People"), by and through Michael N. Feuer, the City Attorney of Los Angeles, bring this civil law enforcement action

Screen Scraping

- Breach of contract (e.g., website terms, EULA, API terms)
- CFAA (and equivalent state computer trespass law)
- Direct and contributory copyright infringement; DMCA
- Common law trespass; conversion
- Unfair competition
- Misappropriation

UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA SAN FRANCISCO DIVISION	
CRAIGSLIST, INC., a Delaware corporation,	Case No. CV 12-03816 CRB
Plaintiff,	FIRST AMENDED COMPLAINT FOR:
v.	(1) Breach of Contract
3TAPS, INC., a Delaware corporation; PADMAPPER, INC., a Delaware corporation; DISCOVER HOME NETWORK, INC., a Delaware Corporation d/b/a LOVELY; BRIAN R. NIESSEN, an individual, and Does 1 through 25, inclusive,	(2) Trespass
Defendants.	(3) Misappropriation
	(4) Violations of the Computer Fraud and Abuse Act
	(5) Copyright Infringement
	(6) Contributory Copyright Infringement
	(7) Federal Trademark Infringement
	(8) Federal False Designation of Origin
	(9) Federal Dilution of a Famous Mark
	(10) Federal Cyberpiracy Prevention
	(11) California Trademark Infringement
	(12) Common Law Trademark Infringement
	(13) California Unfair Competition
	(14) California Comprehensive Computer Data Access and Fraud Act
	(15) Aiding and Abetting Trespass
	(16) Aiding and Abetting Misappropriation
	(17) Accounting
	DEMAND FOR JURY TRIAL



Contract Issues

WELCOME TO CRAIGSLIST. We hope you find it useful. By accessing our servers, websites, or content therefrom (together, "CL"), you agree to these Terms of Use ("TOU"), last updated December 05, 2013.

LICENSE. If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or "frame" content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

USE. You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, flagging, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited, as are misleading, unsolicited, unlawful, and/or spam postings/email. You agree not to collect users' personal and/or contact information ("PI").

MODERATION. You agree that we may moderate CL access and use in our sole discretion, e.g. by blocking (e.g. IP addresses), deletion, delay, omission, verification, and/or access/account/license termination. You agree not to bypass said moderation, (2) we are not liable for moderating, not moderating, or re-moderating, and (3) nothing we say or do waives our right to moderate, or not. All site rules, [about/prohibited](#), are incorporated herein.

SALES. You agree to pay for your account for [CL fees](#). Unless noted, fees are in US dollars; tax is additional. All fees are nonrefundable, even for posts we remove. We may

USE. You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, flagging, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited, as are misleading, unsolicited, unlawful, and/or spam postings/email. You agree not to collect users' personal and/or contact information ("PI").



Contract Issues

Website “Terms of Use”

WELCOME TO CRAIGSLIST. We hope you find it useful. By accessing our servers, websites, or content therefrom (together, “CL”), you agree to these Terms of Use (“TOU”), last updated December 05, 2013.

LICENSE. If you are 18 or older, we grant you a limited, revocable, nonexclusive, nonassignable, nonsublicensable license to access CL in compliance with the TOU; unlicensed access is unauthorized. You agree not to license, distribute, make derivative works, display, sell, or “frame” content from CL, excluding content you create and sharing with friends/family. You grant us a perpetual, irrevocable, unlimited, worldwide, fully paid/sublicensable license to use, copy, perform, display, distribute, and make derivative works from content you post.

USE. You agree not to use or provide software (except for general purpose web browsers and email clients, or software expressly licensed by us) or services that interact or interoperate with CL, e.g. for downloading, uploading, posting, emailing, search, or mobile use. Robots, spiders, scripts, scrapers, crawlers, etc. are prohibited. We reserve the right to remove any unsolicited, unlawful, and/or spam postings/email. You agree not to

**Craigslist, Inc. v RadPad, Inc., No.
16-01856 (N.D. Cal. Final Judgment
Apr. 13, 2017)**

Computer Fraud and Abuse Act

18 U.S.C. §1030 – Fraud and related activity in connection with computers –

- Provides civil/criminal cause of action for access to a “protected computer” “without authorization or exceeding authorized access,” and obtaining information, causing damage or loss, or furthering a fraud, among other things.
- Many states have parallel or similar computer fraud statutes.
- Must show \$5,000 in damages
- **Key Question:** What is exceeding authorized access? Is breach of terms of use enough?

Scraping of “Public” Website Data

hiQ Labs, Inc. v. LinkedIn Corp., No. 17-16783 (9th Cir. Sept. 9, 2019)

- **Issue:** Crucial question was whether once hiQ Labs received LinkedIn’s C&D letter demanding it stop scraping public LinkedIn profiles, any further scraping of such data was “without authorization” within the meaning of the CFAA
- Appeals court affirmed lower court’s order granting a preliminary injunction barring LinkedIn from blocking hiQ from accessing and scraping publicly available LinkedIn member profiles to create competing business analytic products.
 - Ninth Circuit held that hiQ had shown a likelihood of success on the merits in its claim that when a computer network generally permits public access to its data, a user’s accessing that publicly available data will not constitute access “without authorization” under the CFAA.
 - Court echoed the lower court’s concern that allowing large internet platforms to selectively restrict access to publicly available website data would not necessarily be in the public interest:

Case Law Update

hiQ Labs, Inc. v. LinkedIn Corp., No. 17-16783 (9th Cir. Sept. 9, 2019)

- **Holding:** “[I]t appears that the CFAA’s prohibition on accessing a computer ‘without authorization’ is violated when a person circumvents a computer’s generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. **It is likely that when a computer network generally permits public access to its data, a user’s accessing that publicly available data will not constitute access without authorization under the CFAA.** [emphasis added]. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system. HiQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ’s possibly meritorious tortious interference claim.”

Case Law Update

hiQ Labs, Inc. v. LinkedIn Corp., No. 17-16783 (9th Cir. Sept. 9, 2019)

Implications

- Decision is certainly scraping-positive, and appears to limit reach of CFAA to much scraping activity...but not an absolute green light
 - Other claims can be lurking (e.g., breach of website terms)
- Calculus of any CFAA dispute will turn on nature of data at issue (e.g., public, user data, copyrighted content, data behind a paywall or authentication scheme)
- LinkedIn petitioned for a rehearing *en banc* (i.e., new hearing before 11 panel appeals court). Reserved for cases that conflict with Supreme Court or 9th Circuit precedent or involve questions of “exceptional importance” (F.R.A.P. Rule 35).
 - LinkedIn argued that the *hiQ* decision conflicted with the 9th Circuit *Power Ventures* decision, where the court held that a data aggregator that accesses a website after permission has been explicitly revoked can, under certain circumstances, be civilly liable under the CFAA. That case involved Facebook user data protected by password (where users initially allowed the aggregator permission to access)

Case Law Update *(cont'd)*

***hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-16783 (9th Cir. Sept. 9, 2019)**

Implications

- 9th Circuit denied panel rehearing and rehearing en banc on November 8, 2019
- LinkedIn has asked for more time to petition the Supreme Court for certorari

Robots.Txt

```
# robots.txt
#
# This file is to prevent the crawling and indexing of certain parts
# of your site by web crawlers and spiders run by sites like Yahoo!
# and Google. By telling these "robots" where not to go on your site,
# you save bandwidth and server resources.
#
# This file will be ignored unless it is at the root of your host:
# Used:    http://example.com/robots.txt
# Ignored: http://example.com/site/robots.txt
#
# For more information about the robots.txt standard, see:
# http://www.robotstxt.org/robotstxt.html

User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /INSTALL.php
```

Computer Fraud and Abuse Act

- Did you violate the terms of use?
- Did you get a cease and desist letter?
- Are you circumventing technical measures to block access?
 - Did you conceal who you are by manipulating the “User-Agent” in your http call?
 - Did you check the robots.txt file for the site?
 - Did you pay any attention to what is in it?
 - Did you manipulate IP addresses?
 - Did you take any other actions to hide access?

Copyright

17 U.S.C. §106; 17 U.S.C. §504

- In certain circumstances, automated data collection may infringe upon a site owner's copyright.
- If web scraping leads to the reproduction of any copyrighted content, such activity may give rise to a claim for copyright infringement.
- Special considerations when it comes to User Generated Content Issues
- Circumvention of technological control measures, such as CAPTCHA "I am not a robot" measures to block automated access, could create the basis for liability under the Digital Millennium Copyright Act ("DMCA").

Trespass

- Excessive automated data collection can interfere with the performance of a site.
- To the extent a site crashes, an end-user experiences delays, or a site's operational capacity is otherwise burdened, the data collector may be deemed to have interfered with the site owner's use of its tangible property
- This could constitute a trespass to chattels.

MNPI – Deceptive Conduct

- DOJ – Use of SOX securities fraud statute 18 U.S.C. 1348
 - Section 1348 applied to insider trading (e.g., *U.S. v. Blaszczyk*).
 - (1) a scheme or artifice to defraud;
 - (2) fraudulent intent; and
 - (3) a nexus with a security.
 - Typical elements of 10b-5 insider trading are not applicable
 - No breach of fiduciary duty, personal benefit, or personal knowledge of the benefit.
- July 2018: *U.S. v. Korchevsky* criminal verdict
 - Mail fraud, wire fraud and securities fraud under Section 1348

MNPI – Deceptive Conduct

- SEC/Civil – 10b-5 “scheme” liability

- *SEC v. Dubovoy* (August 2015)

SEC and DOJ charged dozens of traders in scheme to trade on hacked news releases

- Deceptive conduct included hiding intrusions by using proxy servers to mask their identities and by posing as employees
 - Charges: mail & wire fraud, securities fraud, conspiracy, etc.
 - Same scheme charged criminally in *Korchevsky*.
 - 2d Cir: misrepresenting ones identity in order to gain access is plainly “deceptive” under 10b-5

- Advisers Act Rule 204A

- Failure to establish, maintain, and enforce policies and procedures reasonably designed to prevent the misuse of MNPI
 - Recent cases focus on inadequate measures to “enforce” policies and procedures, in light of particularized risks

Insider Trading: Computer Hacking

- ***SEC v. Hong*** (December 2016)
 - Chinese traders charged with hacking into law firm computer networks
 - Deceptive conduct included installing malware, stealing passwords, electronically impersonating IT employee
- Liability when access involved deception/breach of duty

Insider Trading: Misappropriation Theory

- Misappropriation theory prohibits:
 - Any person or entity from trading
 - On basis of material, nonpublic information
 - That has been ***misappropriated*** from a party
 - To whom person owes a duty, or whom he/she deceives
- Liability requires a duty of trust or confidence
 - Duty runs to ***source of info***, not to issuer of securities traded
- Under **Rule 10b5-2**, person has a duty of trust or confidence:
 - When a person **agrees to keep info confidential**;
 - There is history, pattern, or practice of sharing confidences; or
 - Information from his/her spouse, parent, child, or sibling.

Misappropriation Theory: Two Examples

- ***U.S. v. Carpenter*** (2d Cir. 1986)
 - *WSJ* columnist provided advance information about contents of his “Heard on the Street” column
 - Tippees traded on information, as did columnist
 - Advance disclosure violated *WSJ* policy that deemed all news materials to be company property and confidential
 - Columnist was convicted of having misappropriated *WSJ*’s property in breach of his duty to his employer
 - But court noted that *WSJ* itself might have been able to use undisclosed info from “Heard on the Street,” because *WSJ* owned the information and would not have breached duty to anyone

Misappropriation Theory: Two Examples

- ***SEC v. Huang*** (E.D. Pa. 2016), *aff'd* (3d Cir. 2017)
 - Data analyst for Capital One downloaded and analyzed data re: retail purchases made with Capital One credit cards
 - He used this info to predict revenues of retailers who used Capital One cards, and he then traded retailers' stocks
 - Use of info violated Capital One's confidentiality policies
 - Found liable for insider trading on misappropriation theory
 - Breach of duty to his employer
 - Courts concluded that jury could have found credit-card info material even though Capital One card usage represented an average of only 2.4% of retailers' revenues

Insider Trading: Computer Hacking

- **SEC v. Dorozhko** (2d Cir. 2009)
 - Ukrainian programmer hacked into IR company's computer and obtained advance info about earnings reports
 - Hacker traded on MNPI obtained through hack
 - 2d Cir held liability depended on whether hack was “deceptive”
 - “[M]isrepresenting one's identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly ‘deceptive’ within the ordinary meaning of the word.”
 - If deception occurred: potential insider-trading liability
 - If hacker merely exploited weakness in electronic code to gain unauthorized access: perhaps theft, but not “deception”

Accessing Nonpublic Information

- Insider-trading liability will depend on whether method of access to MNPI involved breach of duty or deception
 - Was access to information obtained legitimately?
 - Remember *Dorozhko*, the Ukrainian hacker
 - Insider-trading liability depends on whether access was “deceptive”
 - If you *misrepresent* your ID to gain access to computer system, deception occurred – potential insider-trading liability
 - If you merely exploit weakness in electronic code to gain unauthorized access: perhaps no deception involved
 - But might be theft

Accessing Nonpublic Information (*cont'd*)

- Whether access involved deception/breach of duty (*cont'd*)
 - Violation of website's Terms of Use
 - Is it deception?
 - Will evasions of technological restrictions be deceptive?
 - If user misled website by masking or rotating its IP address, deception involved?
 - Is it a breach of duty?
 - If user agrees to abide by use restrictions, but does not do so?
 - Violation of contract with owner of information
 - Deception or breach of duty if user pays owner for access to information, but uses information in ways or for purposes that contract does not allow?

Contracts with Source/Owner of MNPI

- Contract between would-be user of MNPI and owner of info
 - If usage is in accordance with contract terms/limitations, perhaps no misappropriation, because owner of MNPI has not been deceived/misled
 - Remember *Carpenter*. 2d Cir. noted that *WSJ* or its parent (Dow Jones) might have been able to trade on advance info from “Heard on the Street,” because they owned the info – no breach of duty
 - Perhaps Capital One could have traded on credit-card info?
 - But does owner of info have duty to anyone?
 - Any duty to its own customers to keep info confidential and not use it except for certain purposes?
 - If so, does person/company that makes contract w/owner know about this duty and about any breach by owner?

Contracts with Source/Owner of MNPI

- Contract with owner of information (*cont'd*)
 - Even if owner of info does not breach any duty, contracting party might have other risk of liability even if no insider trading
 - NY's Martin Act authorizes NY AG to sue based on unfairness
 - Information disparity suffices; breach of duty/fraud not needed
 - NY AG has threatened to use Martin Act re insider trading
 - Thomson Reuters/U. Mich. settlement: Thomson agreed to stop selling to priority subscribers early access to consumer-confidence survey
 - 18 large B/Ds agreed to stop responding to buy-side firms' surveys seeking analyst sentiment
 - PR Newswire, Business Wire, and Marketwired agreed to require subscribers to certify they would not do high-frequency trading with info received from outlets' direct data feeds

Contracts with Source/Owner of Info

- Contract with owner of information (*cont'd*)
 - Also need to consider EU Market Abuse Regulation
 - EU regulation can apply to transactions anywhere in world
 - Test is whether security is *admitted for trading on EU markets*
 - If security is traded in EU, place of transaction involving MNPI is irrelevant
 - If U.S. trader uses MNPI in transaction with U.S. counterparty on U.S. market, EU Reg applies if security is also traded in EU

Contracts with Source/Owner of Info

- Contract with owner of information (*cont'd*)
 - EU rules on insider trading differ radically from U.S. rules
 - EU prohibits use of material, nonpublic information
 - Applies to anyone who knew or should have known that material information was nonpublic
 - Defenses available in U.S. are not available in EU
 - Irrelevant whether discloser had duty not to disclose
 - Irrelevant whether discloser received a personal benefit
 - Irrelevant whether recipient owed duty to discloser not to use or disclose the information
 - Under EU rules, if you know or should have known you have MNPI, you cannot use it – period

Acquiring Data from Third Parties

Can I reduce my risk
by hiring a third party
to do this for me?

Acquiring Data from Third Parties – Diligence

- What might be acceptable risk to the vendor may not be acceptable risk for you.
- Technology and business models are way ahead of the law; creativity is high; “safe” practice standards do not exist and the urge to differentiate and add value is pressing.
- Contractual protection may not be enough to shield one from liability. It certainly is not enough to shield from litigation and adverse publicity.

Acquiring Data from Third Parties – Diligence

- Trend, led by the FTC, for expanded vendor diligence and oversight.
- The “WSJ” Test
- Legal “Flow Through” Liability
- Agency Relationships

Acquiring Data from Third Parties

- The Due Diligence Process:
 - Ask the questions in writing; get the answers in writing.
 - Document who is providing the answers and why it is reasonable to accept their responses.
 - Follow up; if it doesn't sound right, it probably isn't.
 - Spot-check the data.
 - Don't use the data other than as provided for in the contract.

Acquiring Data from Third Parties

- The Due Diligence Process: *(cont'd)*
 - Get appropriate contractual reps/warranties/indemnities.
 - Make sure there is at least annual recertification
 - Consider other triggers for recertification as well:
Change of control, MAE, etc.
 - Avoid relying on the vendor's legal analysis.

Fundamental Questions

- Who is the vendor? Is it credible, established, respected?
- What are the vendor's data sources?
- Where is the data coming from? Government or private sources?
- What is the nature of the data? What techniques does the vendor use?
- PII? Child PII? Sensitive Information?
- Any MNPI or other “confidential” information? (Spot-check!)
- Is the vendor collecting the same data for anybody else?

Fundamental Questions

- Has there been any litigation involving the vendor or its sources?
- How does the vendor provide the data? Is the vendor a collector, packager, analyzer, aggregator?
- Does the vendor have the right to provide the data to you? Consider requesting documentation and indemnity.
- If using drones, does the vendor employ or contract with drone operators possessing proper commercial licenses acting in compliance with state and federal laws and NTIA best practices?

Fundamental Questions

- Does the vendor spider? If so:
 - Do the targeted websites have restrictive terms of use? Does the vendor check regularly?
 - Does the vendor use technology to simulate the creation of any user accounts?
 - Does the vendor circumvent any “captchas” or similar technologies?
 - Does the vendor respect the “robots.txt” parameters?
 - Does the vendor identify its “User-Agent” in the site logs?
 - How does the vendor structure IP addresses for spidering?
 - Does the vendor throttle/pause/alternate times to simulate human interaction?

Recent Events

The Yodlee Letter

Congress of the United States

Washington, DC 20510

January 17, 2020

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, DC 20580

Dear Chairman Simons:

We write to urge the Federal Trade Commission (FTC) to investigate Envestnet Inc. (Envestnet) to determine whether the company's sale of sensitive financial transaction data from tens of millions of Americans violates the FTC Act.

Envestnet operates Yodlee, the largest consumer financial data aggregator in the United States. Financial technology apps, banks, and other companies use Yodlee and other financial data aggregators to access, collect, and analyze transaction data from a consumers' bank, credit card, and other financial accounts with the consumer's consent. According to Envestnet, Yodlee is used by more than 1,200 companies, including 15 of the top 20 largest U.S. banks, to offer online personal-finance tools to their consumers.

Envestnet also sells access to consumer data. According to its website, Envestnet can "deliver data from over 21,000 global data sources, so [companies] can easily get the bank, credit card, investment, loans, rewards, and financial account data that [they] need." The company's database includes credit and debit card transactions from tens of millions of consumers, which Envestnet sells to data brokers, who in turn sell that data to hedge funds and other investors that trade based on market trends they observe.

The consumer data that Envestnet collects and sells is highly sensitive. Consumers' credit and debit card transactions can reveal information about their health, sexuality, religion, political views, and many other personal details. And the more often that consumers' personal information is bought and sold, the greater the risk that it could be the subject of a data breach, like the recent breaches at Equifax and Capital One. Envestnet claims that consumers' privacy is protected because it anonymizes their personal financial data. But for years researchers have been able to re-identify the individuals to whom the purportedly anonymized data belongs with just three or four pieces of information.

Consumers generally have no idea of the risks to their privacy that Envestnet is imposing on them. Envestnet does not inform consumers that it is collecting and selling their personal financial data. Instead, Envestnet only asks its partners, such as banks, to disclose this information to consumers in their terms and conditions or privacy policy. That is not sufficient protection for users. Envestnet does not appear to take any steps to ensure that its partners actually provide consumers with such notice. And even if they did, Envestnet should not put the burden on consumers to locate a notice buried in small print in a bank's or apps' terms and conditions or privacy policy, and then find a way to opt out—if that is even possible—in order to protect their privacy.

The FTC has made it clear that companies may not hide important facts about how consumer data is collected or shared in the small print of a privacy policy. This is particularly true when companies have made broad public statements, as Envestnet has done, promising that they will protect consumer privacy. As the FTC noted in its complaint against Sears Holdings in 2009, companies have an obligation to disclose "facts [that] would be material to consumers in deciding to install the software. Sears Holding's failure to disclose these facts, in light of the representations made, was, and is, a deceptive practice."

Though privacy protections should be much stronger, the FTC already has the authority under Section 6(b) of the FTC Act to conduct broad industry reviews. It should do so here in order to determine whether Envestnet's sale of consumers' personal data to third parties without their knowledge or consent is an unfair, deceptive, or abusive act or practice. We also urge the FTC to investigate whether Envestnet and the companies to which it has sold consumer data have the required technical controls in place to protect Americans' sensitive financial data from re-identification, unauthorized disclosure to hackers or foreign spies, or other abusive data practices.

Thank you for your attention to this important matter.

Sincerely,


Ron Wyden
United States Senator


Sherrod Brown
United States Senator


Anna G. Eshoo
Member of Congress

United States Senate
WASHINGTON, DC 20510

January 24, 2019

36

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20530

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street, NW
Washington, DC 20554

Dear Chairman Simons and Chairman Pai:

We write to urge the Federal Trade Commission (FTC) and the Federal Communication Commission (FCC) to broadly investigate the sale of Americans' location data by wireless carriers, location aggregators, and other third parties.

Last year, multiple news reports highlighted the fact that the four major wireless carriers, AT&T, Sprint, T-Mobile, and Verizon, sold their customers' location data to approximately seventy companies, without the explicit knowledge or consent of their customers. After significant negative press coverage, the wireless industry pledged to end these business practices. A recent investigation published by *Motherboard*, however, demonstrated not only that the wireless carriers are still failing to protect their customers' private information, but also that location data can be purchased by stalkers, domestic abusers, and others. It is clear that these wireless carriers have failed to regulate themselves or police the practices of their business partners, and have needlessly exposed American consumers to serious harm.

To that end, we urge the FTC and the FCC to conduct broad investigations, as appropriate, into the business partnerships between wireless carriers and location aggregators, including resellers and all downstream buyers of location data. Specifically, your agencies should determine whether wireless carriers or aggregators knew, or should have known, that failing to demand and verify subscriber consent would result in individuals obtaining location data without the respective subscriber's knowledge or consent. We also ask your agencies to require the wireless carriers to notify every American whose location they shared or sold and to identify to those subscribers the specific companies that obtained their location information.

Americans expect that their location data will be protected. The wireless industry has repeatedly demonstrated a blatant disregard for its customers' privacy. It is therefore vital



FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

January 31, 2020

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
U.S. House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Pallone:

I am writing to follow up on my letter of December 3, 2019 regarding the status of the FCC's investigation into the disclosure of consumers' real-time location data. Fulfilling the commitment I made in that letter, I wish to inform you that the FCC's Enforcement Bureau has completed its extensive investigation and that it has concluded that one or more wireless carriers apparently violated federal law.

I am committed to ensuring that all entities subject to our jurisdiction comply with the Communications Act and the FCC's rules, including those that protect consumers' sensitive information, such as real-time location data. Accordingly, in the coming days, I intend to circulate to my fellow Commissioners for their consideration one or more Notice(s) of Apparent Liability for Forfeiture in connection with the apparent violation(s).

Please let me know if I can be of any further assistance.

Sincerely,

Ajit V. Pai

The New York Times

FCC Plans to Take Action Over Wireless Real-Time Location Data Disclosures

By Reuters

Feb. 3, 2020



WASHINGTON — U.S. Federal Communications Commission (FCC) Chairman Ajit Pai said on Friday the telecommunications regulator plans to take action against at least one unnamed wireless carrier over the apparent unauthorized sale of real-time location data from users.

The FCC said in May 2018 it was referring reports that a website flaw could have allowed the location of mobile phone customers to be tracked to its enforcement bureau to investigate. In a letter to Congress on Friday, Pai said the FCC's enforcement bureau "has concluded that one or more wireless carriers apparently violated federal law."

FCC Commissioner Jessica Rosenworcel said on Friday it was a "shame" the FCC took so long to act on what she called reports that "shady middlemen could sell your location within a few hundred meters based on your wireless phone data." She added, "It's chilling to consider what a black market could do with this data."

About Us

- › [Mission Statement](#)
- › [What we do](#)
- › [Organisational Structure](#)
- › [Data Protection Legislation](#)
- › [Our International Work](#)
- › [Careers](#)

Data Protection Commission launches Statutory Inquiry into Google's processing of location data and transparency surrounding that processing

04th February 2020

The Data Protection Commission, in its role as Lead Supervisory Authority for Google, has received a number of complaints from various Consumer Organisations across the EU, in which concerns were raised with regard to Google's processing of location data. The issues raised within the concerns relate to the legality of Google's processing of location data and the transparency surrounding that processing. As such the DPC has commenced an own-volition Statutory Inquiry, with respect to Google Ireland Limited, pursuant to Section 110 of the Data Protection 2018 and in accordance with the co-operation mechanism outlined under Article 60 of the GDPR. The Inquiry will set out to establish whether Google has a valid legal basis for processing the location data of its users and whether it meets its obligations as a data controller with regard to transparency.

◆ WSJ NEWS EXCLUSIVE | POLITICS

Federal Agencies Use Cellphone Location Data for Immigration Enforcement

Commercial database that maps movements of millions of cellphones is deployed by immigration border authorities

By Byron Tau and Michelle Hackman

Feb. 7, 2020 7:30 am ET

WASHINGTON—The Trump administration maps the movements of millions of cellphones for border enforcement, according to a report by The Wall Street Journal.

The location data is drawn from a commercial database and e-commerce, for which the government pays.

The Department of Homeland Security uses the data on immigrants and others who may be in the country without documents.

U.S. Immigration and Customs Enforcement officials identify immigrants who were in the country without documents.

The New York Times

Opinion

The Government Uses 'Near Perfect Surveillance' Data on Americans

Congressional hearings are urgently needed to address location tracking.

By The Editorial Board

The editorial board is a group of opinion journalists whose views are informed by expertise, research, debate and certain longstanding values. It is separate from the newsroom.

Last year, a Times Opinion investigation found that claims about the anonymity of location data are untrue since comprehensive records of time and place easily identify real people.

OCIE Exam Priorities

- On January 7, 2020, OCIE released its 2020 Examination Priorities identifying ‘alternative data’ as a focus.
 - Innovations and advancements in financial technologies, methods of capital formation, market structures, and investor interfaces continue to grow at a rapid pace. For example, registered firms are increasingly using new sources of data, often referred to as “alternative data” by the industry that, among other things, may drive investment decision-making.
 - OCIE remains focused on keeping abreast of these developments, and examinations will focus on firms’ use of these data sets and technologies to interact with and provide services to investors, firms, and other service providers and assess the effectiveness of related compliance and control functions.

OCIE Exams (cont'd)

- We are now seeing written follow-up questions on Big Data in OCIE exams (in addition to oral questions). Here are some examples:
 - Please describe Registrant's processes and procedures for identifying, vetting, testing, implementing, and monitoring entities or individuals that provide or make available information that is utilized in the investment decision making process pursuant to a contractual agreement (collectively "Data and Research Providers"). Data and Research Providers would include but not be limited to research consultants, expert networks, data aggregators, survey companies, entities selling data from their own business operations (sometimes called "business exhaust data"), entities that assist with the extraction, transformation and loading of data (commonly referred to as ETL), broker-dealers supplying research or data, and providers of market data, web scraped data, consumer spending data, satellite images, supply chain data, flight tracking data, geolocation data, factor analysis, political intelligence and analyst reports.

OCIE Matters (cont'd)

- Please describe Registrant's data collection efforts of internal staff or affiliated entities to make available or structure data that is utilized for Registrant's investment activities; Registrant should describe any collection of data from other parts of the Registrant or their affiliates' businesses in the investment decision-making process. Registrant should also describe any collection of data by employees through direct efforts of the Registrant or its employees (e.g., web scraping, surveys, channel checking, etc.).
- Please describe Registrant's allocation and availability of data across clients and portfolio managers.

Insider Trading Updates

- Insider Trading Prohibition Act (H.R. 2534)
 - Passed overwhelmingly by the House on 12/5/2019
 - Proposed concept of “wrongful” use of information includes data protection statutes

H.R. 2534 – proposed Insider Trading Prohibition Act

- “(1) STANDARD.—For purposes of this section, trading while aware of material, nonpublic information under subsection (a) or communicating material nonpublic information under subsection (b) is wrongful only if the information has been obtained by, or its communication or use would constitute, directly or indirectly—
 - “(A) theft, bribery, misrepresentation, or espionage (through electronic or other means);
 - “(B) a violation of any Federal law protecting computer data or the intellectual property or privacy of computer users;

Insider Trading Updates *(cont'd)*

H.R. 2534 – proposed Insider Trading Prohibition Act (cont'd)

- “(C) conversion, misappropriation, or other unauthorized and deceptive taking of such information; or
- “(D) a breach of any fiduciary duty, a breach of a confidentiality agreement, a breach of contract, a breach of any code of conduct or ethics policy, or a breach of any other personal or other relationship of trust and confidence for a direct or indirect personal benefit (including pecuniary gain, reputational benefit, or a gift of confidential information to a trading relative or friend).

Insider Trading Updates

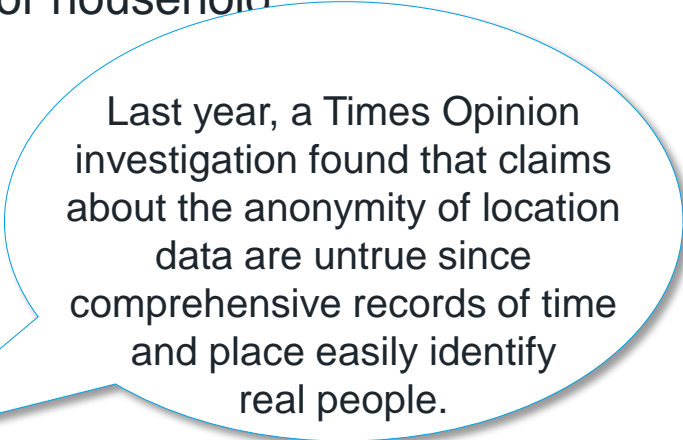
H.R. 2534 – proposed Insider Trading Prohibition Act

- “(2) KNOWLEDGE REQUIREMENT.—It shall not be necessary that the person trading while aware of such information (as proscribed by subsection (a)), or making the communication (as proscribed by subsection (b)), knows the specific means by which the information was obtained or communicated, or whether any personal benefit was paid or promised by or to any person in the chain of communication, so long as the person trading while aware of such information or making the communication, as the case may be, was aware, consciously avoided being aware, or recklessly disregarded that such information was wrongfully obtained, improperly used, or wrongfully communicated.

The California Consumer Privacy Act

- Personal information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes...the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household

Section 1798.140(o)(1)



Last year, a Times Opinion investigation found that claims about the anonymity of location data are untrue since comprehensive records of time and place easily identify real people.

The New York Times

Proskauer >>

New (Feb. 7, 2020) Proposed Regs Under CCPA

- **Section 999.302.** Guidance Regarding the Interpretation of CCPA Definitions

(a) Whether information is “personal information,” as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that “identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.” For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be “personal information.”

Selected Examples – Section 1798.140(o)(1)

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, internet protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(x) "Unique personal identifier" defined as a persistent identifier that can be used to recognize a consumer...or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol... or similar technology; customer number, ... or other forms of persistent or probabilistic identifiers that can be used to identify a particular consumer or device.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

(G) Geolocation data.

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(m) Infer/Inferences defined as the "derivation of information, data, assumptions, or conclusions from facts, evidence, or another source of information or data."

Deidentification and the CCPA

- **Section 1798.140(o)(3):** “Personal information” does not include consumer information that is deidentified or aggregate consumer information.
- **Section 1798.145(a)(5):** The obligations imposed on businesses by this title shall not restrict a business’ ability to:...(5) Collect, use, retain, sell, or disclose consumer information that is deidentified or in the aggregate consumer information.
- **Proposed Regulation 999.323:** “If a business maintains consumer information that is deidentified, a business is not obligated to provide or delete this information in response to a consumer request or to re-identify individual data to verify a consumer request.”

Deidentification and the CCPA (cont'd)

- **Section 1798.140(h):** “Deidentified” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information...
 - implemented technical safeguards that prohibit reidentification
 - implemented business processes that prohibit reidentification
 - implemented business processes to prevent release of deidentified information
 - makes no attempt to reidentify the information.
- **Section 1798.140(a):** “Aggregate consumer information” means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device.
- But remember, Personal Information includes information which “is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.”

Deidentification and the CCPA (cont'd)

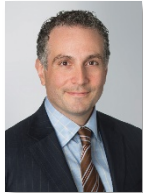
- **Question:** How can information which is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer (i.e., personal information) ever be information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer (e.g., de-identified or aggregate)?

Contacts

Hedge Funds



Robert G. Leonard
212-969-3355
rleonard@proskauer.com



Michael F. Mavrides
212-969-3670
mmavrides@proskauer.com



Christopher M. Wells
212-969-3600
cwells@proskauer.com

Technology, Media & Telecommunications



Jeffrey Neuburger
212-969-3075
jneuburger@proskauer.com

Enforcement and Securities Litigation



Joshua Newville
212-969-3336
jnewville@proskauer.com



Samuel J. Waldon
202-416-6858
swaldon@proskauer.com

Proskauer 2020 Winter Regulatory Update - OCIE “Big Data” Interview Questions

Lines of questioning by OCIE regarding Big Data during interviews:

- Sourcing
 - Understanding the business/use case for the data set
 - Whether the information was prepared for the firm specifically or gathered generally and available to anyone who wished to purchase it (which goes to “agency” issue)
- Vetting
 - Description of the people involved in conducting diligence
 - Understanding the type of diligence (both initial and ongoing)
 - Understanding the compliance program at the provider
 - Process for documenting the diligence
 - Contractual terms – negotiation on reps/warranties/indemnities
 - Once a data set is procured, understanding the processes (if any) for testing the data sets for MNPI or PII (personally identifiable information)
 - Turning down a vendor/terminating a vendor due to MNPI, PII or other matters
- Usage
 - Data set access
 - How it is used in portfolio decision-making
- Web-scraping
 - Groups/individuals
 - Internal v. external
 - Understanding the who/what/when of the collection process
 - Understanding the processes they follow (documented or undocumented)
 - Compliance/Legal
 - Awareness of website terms of service
 - Going around/through website “click thru”, captcha, etc.
 - Awareness of scraping impact on websites
 - Reviewing data gathered for MNPI or PII
 - Compliance/legal interaction with data collection team

Hedge Fund Firms – What Do You Need to Consider Under the CCPA?

December 11, 2019

The California Consumer Privacy Act of 2018 (CCPA) will take effect on January 1, 2020, and hedge fund firms may be subject to the CCPA even if they are already compliant with the Gramm-Leach-Bliley Act (GLBA), do not have a place of business in California or do not target California consumers or businesses as those terms are broadly defined in the CCPA.

The CCPA is an expansive new privacy law that gives "consumers" (broadly defined as natural persons who are California residents — potentially including current and prospective hedge fund clients and investors and personnel and job applicants of the hedge fund firm) four basic rights in relation to their personal information:[1]

1. the **right to know**, through a general privacy policy and with more specifics available upon request, what personal information a business has collected about them, from where it was sourced, for what it is being used, whether it is being disclosed or sold, and to whom it is being disclosed or sold;
2. the **right to "opt out"** of allowing a business to sell its personal information to third parties (or, for consumers who are under 16 years old, the right not to have its personal information sold absent its, or its parent's, opt-in);
3. the **right to have a business delete its personal information**, with some exceptions; and
4. the **right to receive equal service and pricing from a business**, even if it exercises its privacy rights under the CCPA.

To whom does the CCPA apply?

Only "Covered Businesses" are within the scope of the CCPA, so hedge fund business must determine whether the fund itself, the fund's manager, general partner, or other similar entities fit within that definition. Covered Businesses are those that:

1. Do business in California;

Practice Tip: Although "doing business in California" is not defined or addressed in the CCPA, the California tax laws describe "doing business" as meeting any one of the following: (1) engaging in any transaction for the purpose of financial gain within California; (2) being

organized or commercially domiciled in California; or (3) having California sales, property or payroll exceed certain threshold amounts which are subject to change each year (payroll threshold for 2018 was \$58,387)).

2. Collect consumer personal information or have it collected on their behalf; and

Practice Tip: The term "consumer" can include a current or prospective client, fund investor, employee and job applicant. This provision may be triggered if hedge funds are using a third party to collect certain client, investor, employee or job applicant personal information on their behalf.

3. Determine the purpose and means of processing that personal information.

In addition to the above requirements, to be considered a Covered Business, an entity must also satisfy at least one of the following elements:

1. Have annual gross revenue of over \$25 million;

Practice Tip: The annual \$25 million gross revenue threshold includes parent companies and subsidiaries sharing the same branding even if they do not meet the applicable threshold themselves. The revenue provision needs additional clarification as drafted, and it is anticipated that this provision will be subject to litigation in the courts. Many companies are erring on the side of over-inclusion of revenue.

2. Buy, receive, sell or share the personal information of 50,000 or more consumers, households or devices for commercial purposes, or
3. Derive 50% or more of annual revenue from selling consumers' personal information.

How does GLBA compliance affect the CCPA?

The CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the GLBA and implementing regulations. Investment advisers registered with the U.S. Securities and Exchange Commission are subject to the GLBA. However, the GLBA exception does not categorically exempt investment advisers and other financial institutions from the CCPA. Rather, the GLBA exception carves out specific categories of data. This carve-out begs the question of what information falls into this exception and what information hedge fund businesses collect that fall outside the scope of the GLBA exception.

The GLBA protects non-public personal information (NPI) of consumers, meaning information that is not publicly available that, in connection with a financial product or service, (i) the consumer provides, (ii) results from a transaction, or (iii) the entity otherwise obtains. Notably, the GLBA applies to "consumers," meaning individuals, as opposed to entities. However, the GLBA may

protect individuals affiliated with entities, such as authorized signatories. NPI could include account balances, credit account data, or even web cookies if collected in association with a financial product. 12 C.F.R. §1016.3(q)(2).

The CCPA is broader than the GLBA with respect to the information to which it applies. Notably, the CCPA applies to ***all personal information relating to*** a consumer (e.g., a current or prospective investor), not just NPI. Hedge fund firms will need to carefully evaluate the nature of the information they obtain and their relationship with individuals with whom they do business, because information may be considered NPI if "otherwise obtained" in connection with providing a financial service.

The CCPA is also broader than the GLBA regarding whose information it applies to, though that breadth has been limited by recent amendments that are expected to be signed into law by the California governor. Further, where the GLBA is limited in protecting entity-affiliated individuals, such as employees or business-to-business contacts, Assembly Bill 25 and Assembly Bill 1355 amend the CCPA to address these issues: the former exempts certain employment-related data[2] and the latter exempts personal information collected in certain business-to-business transactions. Neither amendment provides complete exemptions, however, leaving in place some notice and opt-out obligations to consider.

Thus, the CCPA covers information outside the scope of the GLBA, which would be any personal information relating to a consumer or household that is not NPI and not covered by a separate CCPA exception. This information could include marketing data and statistics or data scraped or bought outside of the ordinary relationship with the individual.

Practice Tip: Assuming that the hedge fund firm meets the CCPA thresholds and collects information that is not NPI covered by the GLBA, it should decide using a risk-based assessment whether to implement CCPA compliance across all personal information or to identify the personal information that does not fall under the GLBA and is for California residents and treat that information differently. Specific notices and means of identifying California residents would need to be operationalized and put into practice with respect to this subset of personal information that is covered by the CCPA.

How should hedge fund firms handle alternative data sources?

Whether scraping data or purchasing data from third party vendors, hedge fund firms should apply the same CCPA principles to such data. The CCPA does not apply to anonymized, aggregated, or deidentified data collected by a business, but firms may need to dedicate more resources to evaluating whether such information is truly free from personal information. Among other things, they should consider negotiating representations regarding such data in agreements with data providers. Firms may be wondering how to handle opt-out requests with regard to their alternative data sources to the extent any data contains personal information. No guidance has been issued on

these matters yet, but presumably firms would not have to honor such requests where the data is fully anonymized or deidentified.

If the CCPA applies, what should I do?

If the CCPA does apply to your firm, you should:

1. *Understand how personal information flows in and out of your business:* Create an inventory, or data map, of all personal information that you collect, use, disclose, or sell pertaining to California residents, households and devices, as well as sources, storage locations, usage and third parties with whom it is shared. Determine whether you are "selling" any personal information, in which case other steps must be taken.

Practice Tip: A "sale" or "selling" of personal information under the CCPA includes "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means" the personal information of a California resident to another business or third party for "monetary or other valuable consideration." This is an extremely broad definition and even the sharing of personal information to third-party and networks through cookies may constitute a sale.

2. *Revise privacy notices and websites:* Disclose categories of personal information collected and how data is used, shared and sold. Clearly describe the rights of California residents, including: (a) the right to access personal information; (b) the right to delete personal information; and (c) the right to opt out of the sale of personal information.

3. *Prepare to receive, process and respond to California residents' request:* Create internal procedures and train applicable personnel.

4. *Do not discriminate against clients, investors, employees, job applicants and other consumers by virtue of their privacy settings:* Businesses cannot deny goods or services, charge different prices for goods or services, or provide a different quality of goods or services to those consumers who exercise their privacy rights.

5. *Add required provisions to contracts with service providers:* To avoid liability under the CCPA for the actions of your service providers, you can include the following prohibitions in your agreements with service providers, provided that you do not have actual knowledge, or reason to believe, that the service provider intended to commit the violation in question:

- a. The service provider may only retain personal information "for the specific purpose of performing the services specified in the contract" or otherwise permitted under the CCPA;
- b. The service provider may only use the personal information "for the specific purpose of performing the services specified in the contract" or otherwise permitted under the CCPA, or;

- c. The service provider may only disclose the personal information "for the specific purpose of performing the services specified in the contract" or otherwise permitted by the CCPA.

How is it enforced?

The CCPA can be enforced through actions brought by the California attorney general and, for certain violations, through private law suits brought by consumers. Note that the California attorney general recently issued proposed rules that would expand obligations regarding initial notices at the collection of personal information, privacy policies, rights regarding sales of personal information, and notice of financial incentives for retention or sale of personal information, amongst other changes. The proposed rules will undergo a comment period in December 2019 and will be enforceable by the attorney general on July 1, 2020.

Please contact Proskauer's Privacy & Cybersecurity team and/or your regular Proskauer contact for more information and to discuss how we can assist you in complying with the CCPA.

[1] "Personal information" is defined, in part, as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Note that the definition of "Personal information" does not include publicly available information or consumer information that is deidentified or aggregate consumer information. CCPA § 1798.140(o).

[2] As of this writing, the employment-related data exemption sunsets on January 1, 2021.

