SIDLEY

MARCH 2, 2018

SIDLEY UPDATE

SEC Issues New Guidance on Cybersecurity Disclosure Requirements

On February 21, 2018, the U.S. Securities and Exchange Commission issued interpretive guidance (the Guidance) to assist public companies in drafting their cybersecurity disclosures in SEC filings. *See* 83 FR 8166 (Feb. 26, 2018). In his public statement accompanying the issuance of this guidance, SEC Chairman Jay Clayton said he believed that "providing the Commission's views on these matters will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors."[1] In this new guidance, the SEC is likely intending to signal how it may focus future enforcement concerning the cybersecurity disclosure obligations of public companies, and their underlying disclosure controls, procedures and certifications.

The new components to the SEC's guidance that all public companies should take into account include the following:

- **Cyber Disclosure Controls and Procedures**. Notwithstanding the fact that there is no specific Regulation S-K line item with respect to cybersecurity, the SEC has made clear that a company's disclosure controls and procedures, per Exchange Act Rule 13a-15, include controls and procedures to ensure that information about cybersecurity risks and incidents is processed and reported to the appropriate personnel to enable senior management to make disclosure decisions and certifications. Companies that support their CEO and CFO certifications regarding the effectiveness of disclosure controls and procedures with subcertifications by direct reports should consider how these subcertifications will need to be revised and expanded.
    - The Guidance specifies that these controls and procedures should:
        - enable companies to identify cybersecurity risks and incidents;
        - assess and analyze their impact on a company's business;
        - evaluate the significance associated with such risks and incidents;
        - provide for open communications between technical experts and disclosure advisors; and
        - make timely disclosures regarding such risks and incidents.

[1] SEC Chair Jay Clayton, "Statement on Cybersecurity Interpretive Guidance" (Feb. 21, 2018), available at https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21.

- **This focus on open communications between "technical experts" and disclosure advisors is new.**

- **Policies to Prevent Insider Trading Based on Nonpublic Cyber Information**. The Guidance stresses the need for companies to consider implementing policies to prevent insider trading on the basis of any material nonpublic cybersecurity-related information. As a result, insider trading policies, codes of ethics and codes of conduct may need to be amended to expressly address information relating to cybersecurity risks and incidents. In addition, controls and procedures with respect to opening and closing trading windows may also need to be revised.
- **Improving Cyber Disclosures**. In general, the Guidance and the accompanying public statements make clear that the SEC and its Staff believe that current company disclosures about cybersecurity risks and incidents can be and must be improved.

The Guidance is the latest in a series of steps taken by the SEC and its Staff to make clear its increasing focus on cybersecurity matters; it both reinforces and expands upon the 2011 guidance issued by the Division of Corporation Finance regarding disclosure obligations relating to cybersecurity risks and incidents. Undeniably, the Guidance is intended to signal that the SEC and its Staff are raising the bar with respect to their expectations about the quality and usefulness of cybersecurity disclosure, and the compliance and governance framework with respect to how cybersecurity risks and incidents are handled. While a grace period can be expected with respect to the transition to the enhanced normative standards outlined in the Guidance—including comment letters on periodic filings by the Division of Corporation Finance—at some point, those expectations will begin to get enforced by the Division of Enforcement.

To be sure, the two Democrat Commissioners, in their separate public statements, qualified their support for the guidance, indicating that it "essentially reiterates years-old staff-level views on this issue"[2] and is simply "rebranded guidance."[3] In Commissioner Jackson's view, "much more needs to be done." Commissioner Stein agreed: "There is so much more we can and should do."

Regardless of the debate among the Commissioners, it is important for companies to consider the spirit and the letter of the Guidance when evaluating their approach to cybersecurity reporting and cybersecurity risk.

Set forth below in more detail is an overview of the Guidance.

OVERVIEW OF RULES REQUIRING DISCLOSURE OF CYBERSECURITY ISSUES

1. Disclosure Obligations Generally; Materiality

Like the 2011 guidance, the Guidance emphasizes that companies "should consider" the materiality of cybersecurity risks and incidents when preparing required disclosures. 83 FR 8166, 8168 (Feb. 26, 2018). The SEC acknowledged that Regulation S-K does not specifically refer to cybersecurity but has interpreted it to include material cyber risks and incidents. In particular, the SEC states that cybersecurity-related disclosures should be considered in companies' periodic reports, registration statements and current reports.

[2] Commissioner Robert J. Jackson, Jr., "Statement on Commission Statement and Guidance on Public Company Cybersecurity Disclosures" (Feb. 21, 2018), available at https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21.

[3] Commissioner Kara M. Stein, "Statement on Commission Statement and Guidance on Public Company Disclosures" (Feb. 21, 2018), available at https://www.sec.gov/news/public-statement/statement-stein-2018-02-21.

Further, the Guidance reinforces that the assessment of disclosure obligations is dependent upon a company's particular circumstances, with thought given to the potential materiality of the identified risk, the importance of compromised information (if any), and/or the impact of an incident on a company's operations, as applicable. *Id*. Materiality, in turn, is dependent upon, among other things, the nature, extent, and potential magnitude of a risk or incident (particularly in relation to compromised information, the business, or the scope of a company's operations), as well as the range of harm (including, for instance, as related to a company's reputation, financial performance, customer/vendor relationships, and/or the possibility of litigation or regulatory investigations or actions). *Id*. at 8168–69.

2. Risk Factors

Regulation S-K's Item 503(c) and Form 20-F's Item 3.D require companies to disclose the most significant factors that make securities investments speculative or risky. *Id*. at 8169–70. The Guidance suggests that companies consider the following factors when evaluating cybersecurity risks for disclosure:

- occurrence, frequency, and severity of prior cybersecurity incidents;
- probability and potential magnitude of cybersecurity incidents;
- adequacy of preventative actions taken to reduce cybersecurity risks and the associated costs;
- aspects of the company's business and operations that give rise to material cybersecurity risks (including industry-specific risks and third-party supplier/service provider risks);
- costs associated with maintaining cybersecurity protections (such as cyber insurance coverage or service provider payments);
- potential for reputational harm;
- existing or pending laws and regulations that may affect the cyber requirements and the associated costs to companies; and
- litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.

The SEC suggests that companies may need to discuss past incidents to provide sufficient context and understanding of cyber risk. For example, the SEC suggests, if a company previously experienced a material denial-of-service attack, it likely would not be sufficient for the company to simply disclose a risk of a denial-of-service incident without mentioning the prior incidents and their consequences.

3. Content and Timing of Disclosures

The SEC provides particular guidance on the content and timing of cyber disclosures. Regarding content, the SEC states that "companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors." *Id*. at 8169. Companies should disclose "cybersecurity risks and incidents that are material to investors, including the concomitant financial, legal, or reputational consequences." *Id*. This includes a "duty to correct" a prior disclosure determined to be untrue or misleading at the time it was made, and a "duty to update" a prior disclosure that becomes materially inaccurate after it is made. *Id*. At the same time, consistent with its 2011 guidance, the SEC cautioned that companies need not and should not provide "detailed disclosures that could compromise cybersecurity efforts" — for instance, by providing a "roadmap" to hackers. *Id*.

On timing, although the SEC recognizes the need for internal investigation and cooperation with law enforcement, the SEC makes clear that such "ongoing internal and external investigation —which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident." *Id*. Thus, such disclosures should be timely and companies should provide them with expediency, though the SEC understands that it may take some time to discern the implications a cybersecurity incident and that some material facts may not be available at the time of the initial disclosure.

4. MD&A of Financial Condition and Results of Operations

Regulation S-K's Item 303 and Form 20-F's Item 5 require companies to discuss their financial condition, changes in financial condition, and results of operations. *Id.* at 8170. The SEC recommends that companies consider:

- costs of ongoing cybersecurity efforts (including enhancements to existing efforts);
- costs and other consequences of cybersecurity incidents or of cybersecurity issues more generally, including, for instance, immediate costs of an incident, loss of intellectual property or competitive advantage, reputational harm, implementation of preventative measures, maintenance of insurance, litigation and regulatory response, remediation efforts, compliance with legislation, etc.; and
- risks of potential cybersecurity incidents.

5. **Description of Business**

According to the Guidance, in connection with Item 101 of Regulation S-K and Item 4.B of Form 20-F, a company "must provide appropriate disclosure" if cybersecurity incidents or risks materially affect its products, services, competitive conditions, or relationships with suppliers or customers. *Id*.

6. Financial Statement Disclosures

The Guidance notes that cybersecurity incidents and risks may affect a company's financial statements. *Id.* For example, cybersecurity incidents may result in expenses related to investigation and breach remediation, loss of revenue, insurance premium increases, or diminished future cash flow. As a result, the SEC "expects" companies to design their financial reporting and control systems to provide reasonable assurance that information regarding the range and magnitude of such impacts would be incorporated into its financial statements in a timely manner.

7. Legal Proceedings

Regulation S-K's Item 103 requires companies to disclose information relating to material pending legal proceedings to which they or their subsidiaries are a party. *Id*. The SEC underscores that this requirement includes any such proceedings that raise cybersecurity issues. For example, if a company experiences a cybersecurity incident involving the theft of customer information and the incident results in material litigation by customers against the company, the company should disclose such litigation.

8. Board Risk Oversight

Regulation S-K's Item 407(h) and Schedule 14A's Item 7 require a company to disclose the extent of its board of directors' risk oversight role, such as how the board administers its oversight function and the board's leadership structure. *Id.* To the extent cybersecurity risks are material, the company should disclose the board's oversight of cybersecurity risks. The SEC notes that disclosures regarding the company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues permit investors to assess how the board is discharging its risk oversight responsibility.

POLICIES AND PROCEDURES

The Guidance also expands on two concepts: disclosure processes and protections against insider trading.

1. Disclosure Controls and Procedures

Exchange Act Rules 13a-15 and 15d-15 require companies to maintain disclosure controls and procedures and evaluate their effectiveness. *Id.* at 8171. The Guidance advises companies to assess whether their disclosure controls and procedures are effective to process and report information regarding cybersecurity risks and incidents, including up the corporate ladder, as appropriate "to enable senior management to make disclosure decisions and certifications" and facilitate insider trading prohibitions. *Id.* In particular, the Guidance indicates that companies should assess whether their controls and procedures enable them to:

- record, process, summarize, and report information related to cybersecurity risks and incidents required to be disclosed in filings;
- identify cybersecurity risks and incidents;
- assess and analyze the impact of cybersecurity risks and incidents on a company's business;
- evaluate the significance associated with such risks and incidents;
- provide for open communications between technical experts and disclosure advisors; and
- ensure timely disclosures regarding such risks and incidents.

2. Insider Trading

The Guidance reminds companies that their directors, officers, and other corporate insiders should be mindful of complying with the laws related to insider trading in connection with material nonpublic information about cybersecurity risks and incidents, including as related to vulnerabilities and breaches. *Id.*8171–72.

The Guidance encourages "companies to consider how their codes of ethics and insider trading policies take into account and prevent trading on the basis of material nonpublic information related to cybersecurity risks and incidents." *Id.* Companies should have policies and procedures in place to prevent trading on the basis of all types of material nonpublic information, including as appropriate information relating to cybersecurity risks and incidents.

3. Regulation FD and Selective Disclosure

Companies should also be sensitive to cybersecurity in the context of evaluating disclosure obligations under Regulation FD and protecting against selective disclosure of material information. *Id.* at 8172. The Guidance provides that companies should not selectively disclose material, nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing the same information to the public and outlines an expectation that company policies and procedures would contemplate this risk.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

Colleen Theresa Brown
Partner
ctbrown@sidley.com
+1 202 736 8465

Paul L. Choi
Partner
pchoi@sidley.com
+1 312 853 2145

Holly J. Gregory
Partner
holly.gregory@sidley.com
+1 212 839 5853

John P. Kelsh
Partner
jkelsh@sidley.com
+1 312 853 7097

Geeta Malhotra
Partner
gmalhotra@sidley.com
+1 312 853 7683

Thomas J. Kim
Partner
thomas.kim@sidley.com
+1 202 736 8615

Edward P. McNicholas
Partner
emcnicholas@sidley.com
+1 202 736 8010

Alan Charles Raul
Partner
araul@sidley.com
+1 202 736 8477

Stephen W. McInerney
Associate
smcinerney@sidley.com
+1 312 853 3766

Clayton G. Northouse
Associate
cnorthouse@sidley.com
+1 202 736 8131

Sidley Privacy and Cybersecurity Practice

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyberlaw. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property and white collar lawyers. We frequently advise regarding HIPAA and Healthcare Privacy issues.

Sidley Corporate Governance and Executive Compensation Practice

Lawyers in Sidley's Corporate Governance and Compliance practice regularly advise corporate management, boards of directors and board committees on a wide variety of corporate governance matters, including corporate responsibility, SEC disclosure, legal compliance, fiduciary duties, board oversight responsibilities and issues arising under Sarbanes-Oxley. Our advice relates to the procedural aspects as well as the legal consequences of corporate and securities transactions and other corporate actions, including takeover defenses, proxy contests, SEC filings and disclosure issues, stock option issues and general corporate law matters. Our broad client base allows us to provide advice regarding best practices and trends in such matters as directors' and officers' responsibilities, board and committee practices, disclosure controls and procedures, internal controls, executive compensation and other matters.

Sidley Securities & Derivatives Enforcement and Regulatory Practice

Sidley's Securities & Derivatives Enforcement and Regulatory group advises and defends clients in a wide range of securities- and derivatives-related matters. With more than 150 lawyers in 10 offices worldwide, we provide comprehensive regulatory, enforcement, and litigation solutions in matters involving the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), self-regulatory organizations (SROs), state attorneys general and state securities regulators. Our team is distinctive in that it combines the strength of nationally recognized enforcement lawyers with the skills of equally prominent counseling lawyers. We work collaboratively to provide our clients with informed, efficient and effective representation.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.

SIDLEY

MARCH 1, 2018

SIDLEY UPDATE

The SEC Speaks 2018: The U.S. Securities and Exchange Commission's Current Priorities and Conference Overview

On Feb. 23 and 24, 2018, senior officials at the annual SEC Speaks conference shared their observations about the current state of financial regulation and the regulatory and enforcement priorities of the Securities and Exchange Commission (SEC). Representatives of each division and each Commissioner, including new Commissioners Hester Peirce and Robert Jackson, offered remarks. Among the topics that received significant attention from nearly all panelists were cryptocurrencies and protection of retail investors.

Chairman Clayton's Remarks on Policymaking Priorities Including Fiduciary Duty

Chairman Jay Clayton kicked off the event with prepared remarks about the Commission, after which he gave additional commentary about the SEC's top policymaking priorities for the upcoming year. The Chairman stated that the SEC will focus on bringing clarity to the standards of care for broker-dealers and investment advisers, following through with already proposed equity market structure reforms,[1] finalizing regulations mandated by the Dodd-Frank Wall Street Reform and Consumer Protection Act and carrying out the SEC's streamlined Regulatory Flexibility Act agenda.

Regarding broker-dealer and investment adviser standards of care, the Chairman explicitly emphasized that the SEC will be making a "big effort" to create "regulatory harmony" between the two standards. The current regulatory structure mandates that brokers meet suitability standards when selling investment products to clients while investment advisers must meet a more onerous fiduciary standard that requires them to act in their clients' best interests. The SEC requested comments on the issue last year and appears poised to work with the Department of Labor and potentially other agencies as the implementation date for the new rule approaches. The rule is scheduled for an implementation date of July 1, 2019.

New Commissioners Jackson and Peirce Describe Their Regulatory Approach and Commissioner Stein Warns About Complex Products

Commissioner Michael Piwowar held question-and-answer sessions with new Commissioners Jackson and Peirce, who were sworn in on Jan. 11. Commissioner Kara Stein gave a separate speech.

[1] This appears consistent with parts of the Department of the Treasury's goals for equity market structure reform. See Sidley update here: https://www.sidley.com/en/insights/newsupdates/2017/10/us-treasury-outlines-initiatives.

- Commissioner Hester Peirce explained her view that economic analysis should be one of the central elements of securities regulation. She also suggested that the SEC should create a separate regulatory framework for "finders" of capital, who currently must register as broker-dealers.
- Commissioner Robert Jackson agreed on the value of using empirical data to inform rulemaking and regulations, but he also noted that some regulations may be appropriate even when their utility may be difficult to precisely quantify, such as insider trading.
- Commissioner Kara Stein expressed concern about the proliferation of complex financial products that are difficult to regulate without market participants and regulators asking threshold questions about whether such products should be sold to investors to begin with.

Updates From the Division of Enforcement

Division of Enforcement officials described their emphasis on cryptocurrencies and the protection of retail investors and noted the following:

- *The establishment of a cyber unit and retail strategies task force*. The Cyber Unit will target cyber-related misconduct through coordination of information sharing, risk monitoring and incident response efforts throughout the SEC. The Retail Strategy Task Force will develop proactive initiatives, leveraging data analytics and technology to identify large-scale misconduct affecting retail investors.
- *The Share Class Selection Disclosure Initiative,* which allows brokers or advisers to self-report failures to disclose conflicts of interest associated with the receipt of 12b-1 fees by the adviser, its affiliates or its supervised persons for investing advisory clients in a 12b-1 fee-paying share class when a lower-cost share class of the same mutual fund was available for the advisory clients. In exchange for self-reporting and certain other action, including reimbursement of harmed investors, the division has agreed to endorse reduced sanctions to the cooperating brokers or advisers and not to seek a civil monetary penalty. The division emphasized that there are benefits to upfront cooperation and self-reporting in other areas of securities regulation and stated that it will continue to work on making those benefits clearer to market participants.
- *Initial Coin Offerings (ICOs).* The division emphasized its balanced approach related to ICOs. For example, in the Munchee Order issued last December, the SEC opted not to impose any civil penalties after the issuer accepted the SEC's settlement offer. Enforcement officials noted that in multiple cases, issuers who were preparing for an ICO voluntarily decided to halt their ICO's progress after coordination and discussion with SEC staff. While the staff expressed that movement toward greater sophistication in the ICO market was a welcome sign, they also stated that attorneys and other regulatory gatekeepers often needed to do a more careful job of advising clients preparing to launch an ICO.

Office of Compliance Inspections and Examinations Leveraging Big Data to Target Exams

The Office of Compliance Inspections and Examinations (OCIE) panels shared important insight into its data-driven strategy for its 2018 National Exam Program Examination Priorities, previously discussed here. OCIE will leverage data from public filings, including Form ADVs, Form BDs and supplemental statements

of income as well as changes in firm manuals, representative disclosures and exam histories to create a framework for modeling risk in the industry.

The panelists described several characteristics that could draw examiners' attention, including (1) firms with a higher percentage of representatives working as independent contractors, (2) firms that have onboarded representatives with disciplinary histories at other firms and (3) firms with unmanaged accounts resulting from representative departures.

In addition, OCIE remains focused on retail investors, with three particular priorities:

- *Roboadvisers.* Examiners will assess the suitability of digital and automated investing platforms based on their ability to tailor advice to the investor's goals and financial situation.[2] OCIE launched a national initiative to review compliance and governance for roboadvisers in areas such as financial modeling, supervision and marketing.
- *Mutual Funds.* OCIE is paying careful attention to the selection of share classes and, in particular, the disclosure of fees and potential conflicts of interest. Firms that do not take advantage of the SEC's recent self-reporting initiative can expect more severe penalties than other firms have faced. Examiners will also target representatives using underperforming funds, funds with liquidity concerns, such as securitized auto loans and consumer debt, and bespoke indices where the adviser may be involved in selecting and weighting components.
- *Exchange-Traded Funds (ETFs).* OCIE has devoted more attention to ETFs as their popularity has continued to grow. Although most ETFs are self-selected, OCIE will examine advisers soliciting "deathwatch ETFs," which raise disclosure issues related to liquidation costs and unsuitable asset spreads.

Updates From the Division of Corporation Finance

Officials from the Division of Corporation Finance discussed new rulemaking initiatives and current issues, with a focus on issues involving cryptocurrencies. The division identified various problems surrounding ICOs and blockchain technology. In particular, the division warned of a multitude of issues involved in the marketing of cryptocurrencies. One of these relates to a potentially false characterization of cryptocurrencies as "utility tokens" in the attempt to evade securities laws. The division warned that cryptocurrencies sold to individuals for the purpose of providing capital returns (with no other potential uses) may be securities even if marketed as utility tokens.

Updates From the Division of Investment Management

The primary topic in the Division of Investment Management discussion centered on cryptocurrencies. Officials noted that over a dozen cryptocurrency strategy funds submitted applications to become registered investment funds in the past year. As a response to put the industry on notice, the division issued a staff letter to the Investment Company Institute outlining the division's concerns surrounding potential new registrations for funds executing cryptocurrency-related strategies. Division officials and members of the

[2] OCIE cited the Division of Investor Management's guidance on roboadvisers, available here.

panel identified concerns of valuation, liquidity, custody, arbitrage (for ETFs) and potential manipulation as fundamental to the structure of investment companies that any potential registered fund must address.

In addition, officials from the division stated that they were working with the Division of Trading and Markets on standards of conduct for brokers and investment advisers. Panelists also noted that while certain funds may desire to use the term "blockchain" in their fund's name, such a change may violate the SEC's rule regarding misleading fund names, according to division officials.

Chief Accountant Advises on Reporting the Effects of Tax Reform

Wesley Bricker, Chief Accountant for the SEC, cautioned public companies against cherry-picking the effects of the Tax Cuts and Jobs Act of 2017 in their financial disclosures. The SEC expects that companies will face some uncertainty, but they should be prepared to report the full effects of the law by the end of 2018.

Until then, Bricker recommended a "triage" approach for reporting, by identifying (1) effects that have taken place, (2) effects that are reasonably likely to occur and (3) effects that have been assessed but have not been quantified. Investors (and the SEC) should be able to track affected items moving through these stages as they review the firm's financial statements during the year.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work or

Stephen L. Cohen
Partner
scohen@sidley.com
+1 202 736 8682

Gerald J. Russello
Partner
grussello@sidley.com
+1 212 839 5716

Jose F. Sanchez
Partner
jose.sanchez@sidley.com
+1 213 896 6103

William Hochul III
Associate
whochul@sidley.com
+1 202 736 8825

Andrew J. Sioson
Associate
asioson@sidley.com
+1 202 736 8351

Securities & Derivatives Enforcement and Regulatory Practice

Sidley's Securities & Derivatives Enforcement and Regulatory group advises and defends clients in a wide range of securities- and derivatives-related matters. With more than 150 lawyers in 10 offices worldwide, we provide comprehensive regulatory, enforcement, and litigation solutions in matters involving the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), self-regulatory organizations (SROs), state attorneys general and state securities regulators. Our team is distinctive in that it combines the strength of nationally recognized enforcement lawyers with the skills of equally prominent counseling lawyers. We work collaboratively to provide our clients with informed, efficient and effective representation.

Investment Funds, Advisers and Derivatives Practice

Sidley has a premier, global practice in structuring and advising investment funds and advisers. We advise clients in the formation and operation of all types of alternative investment vehicles, including hedge funds, fund-of-funds, commodity pools, venture capital and private equity funds, private real estate funds and other public and private pooled investment vehicles. We also represent clients with respect to more traditional investment funds, such as closed-end and open-end registered investment companies (i.e., mutual funds) and exchange-traded funds (ETFs). Our advice covers the broad scope of legal and compliance issues that are faced by funds and their boards, as well as investment advisers to funds and other investment products and accounts, under the laws and regulations of the various jurisdictions in which they may operate. In particular, we advise our clients regarding complex federal and state laws and regulations governing securities, commodities, funds and advisers, including the Dodd-Frank Act, the Investment Company Act of 1940, the Investment Advisers Act of 1940, the Securities Act of 1933, the Securities Exchange Act of 1934, the Commodity Exchange Act, the USA PATRIOT Act and comparable laws in non-U.S. jurisdictions. Our practice group consists of approximately 120 lawyers in New York, Chicago, London, Hong Kong, Singapore, Shanghai, Tokyo, Los Angeles and San Francisco.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.

SIDLEY

BEIJING · BOSTON · BRUSSELS · CENTURY CITY · CHICAGO · DALLAS · GENEVA · HONG KONG · HOUSTON · LONDON · LOS ANGELES · MUNICH · NEW YORK · PALO ALTO · SAN FRANCISCO · SHANGHAI · SINGAPORE · SYDNEY · TOKYO · WASHINGTON, D.C.

SIDLEY

FEBRUARY 12, 2018

SIDLEY UPDATE

Office of Compliance Inspections and Examinations Publishes 2018 Exam Priorities

On February 7, 2018, the Office of Compliance Inspections and Examinations (OCIE) of the U.S. Securities and Exchange Commission (the Commission) released its annual National Exam Program Examination Priorities (Exam Priorities).[1] As has been widely reported, the Exam Priorities' general focus areas include:

- retail investors
- compliance and risks in critical market infrastructure
- oversight of the Financial Industry Regulatory Authority (FINRA) and Municipal Securities Rulemaking Board (MSRB)
- cybersecurity
- anti-money laundering (AML) programs

The majority of these Exam Priorities are not surprising because they reflect the Commission's continued focus on retail investors, conflicts of interest, fee disclosure, cybersecurity, cryptocurrency and AML programs.[2] The Exam Priorities can serve as a roadmap for firms to assess their policies, procedures and compliance programs, and to prepare for OCIE exams. This update outlines and elaborates on each of the Exam Priorities.

As an initial matter, we note that the Exam Priorities include some interesting insights in a discussion of OCIE's guiding principles. For example, in reaffirming OCIE's limited resources, the Exam Priorities make clear that decisions such as which firms to examine and the scope of the exams are guided by a risk-based analysis (rather than in routine cycles). This risk-based approach is driven by rapidly advancing data analysis, including OCIE's proprietary National Examination Analytics Tool (NEAT) developed by its Quantitative Analytics Unit. The insights and skills of OCIE's financial engineers and analysts result in targeted risk analyses to identify potential high-risk examination candidates and risk-based issues to focus OCIE exams.

[1] U.S. Securities and Exchange Commission 2018 National Exam Program Examination Priorities, Office of Compliance Inspections and Examinations, available at https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

[2] See "Testimony on Examining the SEC's Agenda, Operation, and Budget," Chairman Jay Clayton, Washington, D.C., October 4, 2017 ("While I will not go into great detail on all of the principles here, I would like to highlight the second principle, which is particularly important to me – that our analysis starts and ends with the long-term interests of the Main Street investor; or as I call them, 'Mr. and Ms. 401(k)' "), available at https://www.sec.gov/news/testimony/testimony-examining-secs-agenda-operation-and-budget.

A Continued Focus on Retail Investors – what does this mean?

In the past, OCIE often focused on investor-related themes, including conflicts of interest, investment adviser fees and expenses, and the adequacy and accuracy of disclosures. The Exam Priorities continue this trend. OCIE will continue to prioritize the proper disclosure and calculation of fees, expenses and other charges investors pay. OCIE also will continue to devote its attention to valuation, particularly where advisers calculate fees and expenses on asset valuation.

Efforts to safeguard Main Street investors include an emphasis on certain business models or practices, including conflicts of interest that may incentivize the promotion of certain products — specifically those with higher commissions or expense ratios that may be inherently more risky than others and potentially unsuitable for retail investors. In the advisory account context, OCIE will review failures to assign new investment advisory representatives to client accounts when existing representatives depart and changes in account fee structures from commission-based to a percentage of client assets under management. OCIE also will continue its years-long concentration on the fairness and structure of wrap fee programs for various types of retail investors, including best execution and the disclosure of costs included in wrap fee programs for bundled services provided by investment managers. Interestingly, in the context of retail investors, OCIE also notes that it will focus on private fund managers with a "high concentration" of nonprofit organizations and pension funds investing for the benefit of retail investors.

Given the role mutual funds and exchange-traded funds (ETFs) play as primary investment vehicles for retail investing, it is no surprise they are a priority. Indeed, retail funds have been a Commission focus for many years.[3] OCIE continues to highlight advisory personnel that recommend mutual fund share classes with higher sales loads or distribution fees as well as on the risks associated with underperforming mutual funds, mutual funds facing liquidity issues and mutual funds that have inexperienced managers or hold securitized products or other investments that are difficult to value. OCIE will focus on mutual funds and ETFs themselves, including performance and valuation issues, as well as risks of lightly traded ETFs and conflicts related to ETF index providers.

Investment advice offered through automated or digital platforms also continues to be a priority, including the examination of compliance programs' oversight of robo-advisers and similar platforms. Examinations will include review of compliance oversight of the algorithms used to generate investment recommendations, investment marketing materials, protection of investor data and disclosure of conflicts of interest.

Once again, included within the goal of protecting retail investors is continued OCIE focus on never-before-examined investment advisers and examination of advisers that have "elevated risk profiles." Since implementation in 2012 of adviser registration requirements mandated by the Dodd-Frank Wall Street Reform and Consumer Protection Act, the examination of both newly registered advisers and advisers that have not been examined in some time continues to be high on the OCIE priority list. More recently, Chairman Clayton announced that the Commission reassigned approximately 100 broker-dealer examiners

[3] See U.S. Securities and Exchange Commission Division of Investment Management: Report on Mutual Fund Fees and Expenses, December 2000, available at https://www.sec.gov/news/studies/feestudy.htm.

to conduct investment adviser exams and that he expects an increase in investment adviser exams of more than 40 percent this year.[4]

Finally, three other areas that OCIE identified as key for retail investors include: municipal advisors and underwriters, fixed income order allocations, and cryptocurrency and related issues. Compliance by municipal advisors with registration, bookkeeping, supervision and other MSRB requirements will remain in focus. Fixed income order execution will be examined to assess whether broker dealers fulfill their best execution obligations. The Commission also has been vocal about the risk of investment loss, liquidity risk, price volatility and fraud in the cryptocurrency space. Accordingly, cryptocurrency and other blockchain products and services, including initial coin offerings (ICOs), are new focus areas that clearly will receive resources and attention.

Compliance and Risks in Critical Market Infrastructure

Entities that provide critical market infrastructure continue to be an exam priority. With an emphasis on systemically important agencies, clearing agencies can expect OCIE to examine, among other things, their compliance with the Commission's standards for covered clearing agencies and remediation of deficiencies identified in prior exams. Additionally, national securities exchanges can expect requests for internal audits that will serve as a source of information regarding compliance failures and other deficiencies. Other focal points of these exams will include revenue and expense generation, allocation and governance. OCIE further noted that the examination of transfer agents will focus on transfers, recordkeeping and safeguarding funds and securities. Lastly, OCIE will continue to focus on the controls, policies and procedures of Regulation Systems Compliance and Integrity entities (including national securities exchanges and clearing agencies) in order to evaluate their ability to take corrective action in the event of a system anomaly.

FINRA and MSRB

The Commission's oversight of both FINRA and the MSRB will continue throughout 2018. OCIE will scrutinize FINRA's operations and regulatory programs as well as the quality of its broker-dealer and municipal advisor examinations. The MSRB can expect OCIE to evaluate the effectiveness of its internal operational policies, procedures and controls.

Cybersecurity

OCIE will continue to work with firms in all sectors to identify and manage cybersecurity risks and encourage other market participants to engage in this effort as well. OCIE's examinations will focus on cybersecurity governance, risk assessment, access rights and controls, data loss prevention, vendor management, training and incident response. Given the attention that the Commission has paid to cybersecurity in speeches, congressional testimony and stated priorities, registrants should expect cybersecurity to be a component of any Commission exam. Registrants also should take note of the Enforcement Division's creation of a Cyber Unit this past September.[5]

[4] See Chairman Clayton's Testimony at FN 2.

[5] See "Testimony on Examining the SEC's Agenda, Operation, and Budget," Chairman Jay Clayton, Washington D.C., October 4, 2017 ("Cybersecurity is an area that is vitally important to the SEC, our markets and me personally. The prominence of this issue and the heightened focus the agency has on it is the result of various factors, including (1) the increased use of and dependence on data and electronic communications, (2) the greater complexity of technologies present in the financial marketplace and (3) the continually evolving threats from a variety of sources"), available at https://www.sec.gov/news/testimony/testimony-examining-secs-agenda-operation-and-budget. See also The

AML Programs

The Exam Priorities indicate that OCIE's examinations will focus on determining whether financial institutions are adapting their AML programs to address their AML obligations and whether they are filing timely, complete and accurate suspicious activity reports. Examiners will assess whether firms are taking reasonable steps to understand the nature and purpose of customer relationships to comply with their customer due diligence/Know Your Customer responsibilities. OCIE will examine whether financial institutions are conducting timely, robust and independent testing of their AML programs. The 2018 Exam Priorities demonstrate that AML remains a key OCIE focus.[6]

As noted, OCIE's announced priorities should come as no surprise. The Exam Priorities reflect certain concerns and risks Commission officials have expressed over the past few years. Firms should use the roadmap outlined by OCIE to test for, enhance and remediate any suspected deficiencies related to the 2018 OCIE priorities.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work or

Stephen L. Cohen
Partner
scohen@sidley.com
+1 202 736 8682

Elizabeth Shea Fries
Partner
efries@sidley.com
+1 617 223 0388

Laurin Blumenthal Kleiman
Partner
lkleiman@sidley.com
+1 212 839 5525

Fiona A. Philip
Partner
fphilip@sidley.com
+1 202 736 8214

Barry W. Rashkover
Partner
brashkover@sidley.com
+1 212 839 5850

Luke O.I. Frankson
Associate
lfrankson@sidley.com
+1 212 839 5683

Securities & Derivatives Enforcement and Regulatory Practice

Sidley's Securities & Derivatives Enforcement and Regulatory group advises and defends clients in a wide range of securities- and derivatives-related matters. With more than 150 lawyers in 10 offices worldwide, we provide comprehensive regulatory, enforcement, and litigation solutions in matters involving the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), self-regulatory organizations (SROs), state attorneys general and state securities regulators. Our team is distinctive in that it combines the strength of nationally recognized enforcement lawyers with the skills of equally prominent counseling lawyers. We work collaboratively to provide our clients with informed, efficient and effective representation.

Investment Funds, Advisers and Derivatives Practice

Sidley has a premier, global practice in structuring and advising investment funds and advisers. We advise clients in the formation and operation of all types of alternative investment vehicles, including hedge funds, fund-of-funds, commodity pools, venture capital and private equity funds, private real estate funds and other public and private pooled investment vehicles. We also represent clients with respect to more traditional investment funds, such as closed-end and open-end registered investment companies (i.e., mutual funds) and exchange-traded funds (ETFs). Our advice covers the broad scope of legal and compliance issues that are faced by funds and their boards, as well as investment advisers to funds and other investment products and accounts, under the laws and regulations of the various jurisdictions in which they may operate. In particular, we advise our clients regarding complex federal and state laws and regulations governing securities, commodities, funds and advisers, including the Dodd-Frank Act, the Investment Company Act of 1940, the Investment Advisers Act of 1940,

SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity, Stephanie Avakian, Co-Director, Division of Enforcement, Washington, D.C., October 26, 2017, available at https://www.sec.gov/news/speech/speech-avakian-2017-10-26#_edn1.

[6] See "Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance," Kevin W. Goodman, National Associate Director, Broker-Dealer Examination Program, Office of Compliance Inspections and Examinations, Securities Industry and Financial Markets Association, June 18, 2015, available at https://www.sec.gov/news/speech/anti-money-laundering-an-often-overlooked-cornerstone.html.

the Securities Act of 1933, the Securities Exchange Act of 1934, the Commodity Exchange Act, the USA PATRIOT Act and comparable laws in non-U.S. jurisdictions. Our practice group consists of approximately 120 lawyers in New York, Chicago, London, Hong Kong, Singapore, Shanghai, Tokyo, Los Angeles and San Francisco.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.

SIDLEY

JANUARY 16, 2018

SIDLEY UPDATE

Financial Industry Regulatory Authority Issues Its 2018 Examination Priorities

On January 8, the Financial Industry Regulatory Authority (FINRA) released its annual Regulatory and Examination Priorities Letter (Letter) to highlight risks that FINRA believes could adversely affect investors and market integrity. FINRA will focus on these issues during its 2018 broker-dealer examinations. Similar to the previous year's Letter, FINRA's commentary reflects a transparent and cooperative spirit, as it gives serious consideration to feedback received during its current self-evaluation and organizational improvement initiative called FINRA360. The Letter highlights FINRA's efforts to foster an ongoing dialogue with the securities industry and touts FINRA's recent improvements to its examination processes and surveillance systems. The Letter also recognizes that FINRA must work to become a more effective and efficient self-regulatory organization by leveraging the expertise of member firms, especially when it comes to understanding new technologies and financial developments.

The Letter follows closely on the heels of the FINRA Examination Findings Report issued in December. The Examination Findings Report provided summaries of exam findings and common pitfalls to avoid. The findings were largely consistent with the priorities identified at the start of the year in the 2017 Priorities Letter. FINRA should be commended for its efforts in providing firms practical guidance outside of an enforcement context.

As always, firms should use the Letter to review their compliance and supervisory procedures carefully and make any necessary revisions. Firms also should be prepared to address their compliance and supervisory policies in these areas in their upcoming FINRA examinations. The following is a discussion of some of the more important points of the FINRA Letter.

Fraud

As mentioned in last year's Letter,[1] FINRA intends to focus on microcap "pump and dump" schemes, especially those that target elderly investors. FINRA will employ new strategies and new rules, including Rule 2165 (Financial Exploitation of Specified Adults) and amendments to FINRA Rule 4512 (Customer Account Information), in furtherance of this goal. Regarding microcap stocks generally, FINRA will investigate brokers who use their own or their customers' accounts to coordinate trading in microcap stocks with known or unknown counterparties, as this may be a strong indicator of participation in a fraudulent

[1] *See* Sidley Update "FINRA Issues Its 2017 Exam Priorities," available at https://www.sidley.com/en/insights/newsupdates/2017/01/finra-issues-its-2017-exam-priorities.

scheme. Many of these matters are conducted by the Office of Fraud Detection and Market Intelligence (OFDMI). FINRA notes that it has recently made hundreds of referrals to the U.S. Securities and Exchange Commission (SEC) related to microcap schemes and other fraudulent activity such as insider trading, Ponzi-type schemes and issuer fraud.[2]

High-Risk Firms and Brokers

Consistent with last year's Letter is FINRA's focus on identifying high-risk firms and brokers. FINRA will continue to review firms' controls regarding brokers' outside business activities and will also review firms' hiring and supervisory practices for high-risk brokers. The Letter mentions firms' obligation to implement heightened supervisory procedures under Rule 3110 for high-risk individuals and specifically calls attention to firms' remote supervision arrangements, supervision of point-of-sale activities and branch inspection programs.

Consistent with FINRA's goal to identify financial exploitation of the elderly, FINRA intends to examine high-risk brokers' recommendations for speculative or complex products to investors who may not have the necessary sophistication or experience or whose investment objectives are inconsistent with these products. In addition, FINRA will review situations where brokers act as a trustee or hold power of attorney over customer accounts or have future rights to customer assets as a named beneficiary on customer accounts.

Operational and Financial Risks

Business Continuity Planning

FINRA will review firms' business continuity plans (BCPs) to determine how and under what circumstances firms activate their BCPs, how firms classify their systems (critical or secondary) and how firms coordinate with their affiliates and vendors during a business disruption. FINRA will also review firms' recovery plans. Firms should maintain BCPs that are reasonably designed to enable them to meet their existing obligations to customers during a business disruption pursuant to Rule 4370.

Customer Protection and Verification of Assets and Liabilities

In 2018, FINRA will evaluate whether firms have implemented adequate controls to protect customer assets and have kept adequate financial records to verify their ability to protect those assets. FINRA will also assess whether firms maintain sufficient documentation to demonstrate that securities are held free of liens and encumbrances as required by SEC Rule 15c3-3. Focusing on foreign custodians, FINRA will assess whether firms' foreign depositories, clearing agencies and custodial banks are good control locations under Rule 15c3-3 by reviewing the underlying arrangements with foreign custodians.

Technology Governance

In its Letter, FINRA notes that some firms have encountered issues due to faulty implementation of new systems or enhancements to existing systems. In 2018, FINRA will review firms' technology management policies. FINRA observes that maintaining strong controls over technology changes is key for firms to

[2] Although the numbers for 2017 are not publicly available, the FINRA website indicates that in 2016 alone, OFDMI made 785 referrals to the Securities and Exchange Commission (SEC) and others based on fraud surveillance, insider trading, "private investment in public equity" surveillance, and Office of the Whistleblower, and 435 insider trading referrals to the SEC. See referral information, available at http://www.finra.org/industry/ofdmi.

prevent inaccurate, incomplete, untested or unauthorized changes to critical systems and production environments.

Cybersecurity

FINRA has made cybersecurity one of its points of emphasis in recent years by highlighting cybersecurity issues in multiple Exam Priorities Letters,[3] a Special Report,[4] and its recent Examination Findings Report.[5] FINRA's 2018 Letter echoes these previous publications and states that in 2018, FINRA will evaluate the effectiveness of firms' cybersecurity programs to protect sensitive information, reviewing firms' preparedness, technical defenses and resiliency measures, among other things. Firms should refer to the Exam Priorities Letters and the Special Report to assist in establishing effective cybersecurity practices.

Anti-Money-Laundering (AML)

FINRA continues to identify concerns related to firms' AML programs, observing firms' inadequacies in the following areas: procedures to detect and report suspicious transactions, resources for AML monitoring and independent testing required under FINRA Rule 3310(c). FINRA presented its concerns and recommendations in its recent Examination Findings Report.[6] FINRA's Letter also highlights risks related to foreign affiliates conducting transactions in microcap, dual-currency securities and activity related to securities-backed lines of credit.

Liquidity Risk

Another of FINRA's operational/financial points of emphasis is firms' liquidity planning. The Letter states that FINRA will evaluate whether a firm's liquidity planning is appropriate for the firm's business and customers and whether such planning addresses the appropriate scenarios. In addition, FINRA will examine the adequacy of firms' material stress-testing assumptions; FINRA strongly suggests that firms review Regulatory Notice 15-33 for guidance related to developing liquidity management plans.

Short Sales

FINRA has recently observed instances where firms inappropriately charged inflated rates to customers for loans related to short sales. In 2018, FINRA will review whether firms calculate such rates in a manner consistent with their procedures.

Sales Practice Risks

Suitability

Because of the increase in new classes of financial products, FINRA will concentrate its attention on how firms identify products subject to new product approval and the controls that firms put in place to review

[3] *See* FINRA's Exam Priority Letters from 2014-16, available at http://www.finra.org/industry/2014-exam-priorities-letter, http://www.finra.org/industry/2015-exam-priorities-letter and http://www.finra.org/industry/2016-regulatory-and-examination-priorities-letter.

[4] *See* FINRA's Report on Cyber Security Practices, available at http://www.finra.org/file/report-cybersecurity-practices.

[5] *See* Sidley Update "Financial Industry Regulatory Authority Issues Report on Recent Examination Findings," available at https://www.sidley.com/en/insights/newsupdates/2018/01/finra-issues-report-on-recent-examination-findings.

[6] *Id.*

whether personnel make suitable recommendations, especially recommendations involving newly created complex products as well as products such as unit investment trusts.

FINRA also plans to conduct suitability review of firms' practices related to recommendations that investors roll over accounts from employer-sponsored retirement plans to individual retirement accounts because employer plans play such a prominent role in individual retirement planning. In addition, FINRA will review situations where brokers' recommendations require customers to pay unnecessary fees — for example, recommendations that customers purchase products subject to front-end sales charges with a further recommendation shortly thereafter to transfer the holdings to a fee-based advisory account.

Initial Coin Offerings and Cryptocurrencies

FINRA recognizes that regulators have paid significant attention to digital currency assets and initial coin offerings in the past year. FINRA will closely monitor developments in this area, especially if member firms begin to play a role in effecting transactions in such assets.

Use of Margin

FINRA has observed situations where brokers have solicited customers to engage in share purchases on margin but were unaware of the risks. FINRA has also recently observed many situations where brokers entered into margin transactions without their customers' authority. Accordingly, FINRA plans to prioritize the assessment of disclosure and supervisory practices related to margin loans.

Securities-Backed Lines of Credit (SBLOCs)

The use of SBLOCs has rapidly increased — therefore FINRA intends to review firms' compliance with regulatory obligations that apply to them. In particular, FINRA will assess the adequacy of firms' risk disclosures in multiple areas, including disclosures related to a potential market downturn, rising interest rates and tax implications upon liquidation of pledged securities. Separately, FINRA notes that it will review firms' controls to prevent unintended dual pledging of collateral securities.

Market Integrity

Manipulation

The Letter touts FINRA's new surveillance capabilities developed to detect market manipulation. For example, FINRA recently launched the Cross Market Auction Ramping surveillance system, which leverages machine-learning techniques to identify aggressive and dominant trading surrounding the open or close. FINRA also enhanced its Cross Market Marking the Open and Close and Cross Market Layering surveillance systems for deployment in 2018. FINRA intends to further incorporate machine-learning techniques to develop new surveillance systems as markets evolve.

In 2018, FINRA will launch two new report cards to assist member firms in detecting and preventing potential manipulation:

- The Auto Execution Manipulation Report Card highlighting instances in which a market participant uses non-bona fide orders to move the national best bid and offer (NBBO)
- The Alternative Trading System (ATS) Cross Manipulation Report Card identifying instances in which a market participant engages in potential manipulation of the NBBO to modify midpoint prices on an ATS

FINRA expects its report cards to be integrated into firms' compliance and supervisory reviews and that any potential violations and deficiencies be addressed.

Best Execution

FINRA intends to expand its best execution surveillance program to assess the degree to which firms provide price improvement when routing customer orders for execution or when executing internalized customer orders. FINRA will soon be able to analyze frequency and degree of price improvement provided by brokers compared to other execution venues.

In 2018, FINRA will continue to review how brokers manage the conflict of interest that exists between the duty of best execution and brokers' financial interests. Part of this review will include whether broker-dealers' procedures provide for a regular and rigorous evaluation of execution quality. FINRA also will expand execution quality review to include Treasuries, which were required to be reported to FINRA's Trade Reporting and Compliance Engine (TRACE) beginning on July 10, 2017.

Regulation SHO

FINRA plans to place an increased focus on firms' practices related to Rule 201 of Regulation SHO, which requires firms to develop policies and procedures to prevent the execution or display of a short sale order at a price that is equal to or less than the national best bid when a short sale circuit breaker is in effect for a National Market System security. Firms should develop an appropriate supervisory system to comply with Rule 201 or to determine whether short sale activity in which they participate qualifies for a Rule 201 exemption.

Fixed Income

FINRA began surveillance of Treasury data in 2017, following the commencement of trade reporting of Treasuries to TRACE. FINRA is now able to identify instances of late reporting, failing to report interdealer trades, misreporting of interdealer trades and inaccurate execution time reporting. As such, FINRA will expand examinations to include Treasury securities when reviewing for complete, timely and accurate reporting of TRACE-eligible securities.

FINRA announced that it expects to launch a new Fixed Income Mark-up Report Card. The Report Card will provide information to firms (e.g., median/mean percentage markups for each firm) and to the industry based on certain criteria such as investment rating and length of time to maturity. This is a welcome development because until now firms, in some instances, have been made aware of FINRA determinations of unreasonable markups only in an examination and/or enforcement setting. The provision of this information combined with the new FINRA/Municipal Securities Rulemaking Board markup disclosure rules should serve as a significant benefit to the investing public and industry participants.

Options

FINRA developed new surveillance systems in 2017 to detect potential front-running in correlated options products and will remain focused on this area in 2018. FINRA will also focus on "marking the close" schemes where individuals post orders immediately prior to market close with the intent to affect the NBBO at the end of the trading day. In addition, FINRA will conduct reviews of potential violations of Securities Exchange Act (SEA) Rule 14e-4, which governs partial tender offers.

Market Access

FINRA will maintain focus on broker-dealers' compliance with SEA Rule 15c3-5 (the Market Access Rule). FINRA's Letter instructs firms to review the Examination Findings Report[7] for additional information about FINRA's observations regarding concerns and effective practices related to Market Access Rule issues.

ATS Surveillance

FINRA will review ATSs' supervisory systems, continuing to focus on reviews/examinations opened because of surveillance alerts related to ATS activity. FINRA notes that as registered broker-dealers and FINRA members, ATSs must maintain supervisory systems that are reasonably designed to achieve compliance with applicable laws and regulations.

Conclusion

Although FINRA's Letter appears to reflect a cooperative tone, it is nonetheless important for firms to review whether their compliance programs incorporate guidance from the Letter and other recent FINRA publications. As reflected in the FINRA Examinations Finding Report, its exam findings in 2017 closely mirrored the issues identified in the 2017 Priorities Letter. Firms should review their policies and procedures in each of the priority areas and should make revisions where appropriate in preparation for their next examination.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work or

James Brigagliano
Partner
jbrigagliano@sidley.com
+1 202 736 8135

W. Hardy Callcott
Partner
hcallcott@sidley.com
+1 415 772 7402

Kevin J. Campion
Partner
kcampion@sidley.com
+1 202 736 8084

Michael D. Wolk
Partner
mwolk@sidley.com
+1 202 736 8807

Timothy B. Nagy
Counsel
tnagy@sidley.com
+1 202 736 8054

Andrew J. Sioson
Associate
asioson@sidley.com
+1 202 736 8351

Sidley Securities & Derivatives Enforcement and Regulatory Practice

Sidley's Securities & Derivatives Enforcement and Regulatory group advises and defends clients in a wide range of securities- and derivatives-related matters. With more than 150 lawyers in 10 offices worldwide, we provide comprehensive regulatory, enforcement, and litigation solutions in matters involving the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), self-regulatory organizations (SROs), state attorneys general and state securities regulators. Our team is distinctive in that it combines the strength of nationally recognized enforcement lawyers with the skills of equally prominent counseling lawyers. We work collaboratively to provide our clients with informed, efficient and effective representation.

[7] *Id.*

SIDLEY

JANUARY 4, 2018

SIDLEY UPDATE

Financial Industry Regulatory Authority Issues Report on Recent Examination Findings

On Dec. 6, the Financial Industry Regulatory Authority (FINRA) published its "Report on FINRA Examination Findings" (Report). The Report highlights recent examination findings that FINRA deems to be particularly important due to market impact or frequency of occurrence. The Report describes particular compliance challenges and best practices to deal with these issues.

The determination to provide this type of feedback to firms en masse was prompted by the FINRA360 initiative of CEO Robert Cook. In today's regulatory environment, it is rare for examiners to share best practices, provide guidance or assist member firms in complying with FINRA rules and federal and state securities laws — over time, the examination process has become an enforcement-focused enterprise. FINRA should be commended for making the effort to provide guidance outside of the enforcement context, and we hope to see more of it.

Firms should consider this guidance seriously. A firm not adopting this guidance should ensure that it is able to demonstrate that its procedures are equally effective.

The following summarizes the topics outlined in the Report and focuses on FINRA's remarks regarding best practices.

Cybersecurity

FINRA characterizes cybersecurity as one of the principal operational risks facing broker-dealers.[1] In its Report, FINRA lists areas of general cybersecurity weakness, including controls related to accessing firm systems and management of vendors who handle firms' sensitive information. FINRA notes that small- and medium-size firms have not begun to utilize robust data-loss prevention tools and have not consistently segregated responsibilities for requesting and approving cybersecurity changes. FINRA also notes that branch offices have faced greater challenges in managing cybersecurity risks, such as ensuring password security and updating antivirus software.

Firms with the most effective cybersecurity policies generally feature strong governance structures that facilitate escalation of issues to the appropriate levels for resolution. As examples of best practices, FINRA

[1] FINRA has emphasized the importance of firms' managing of cybersecurity risks in past Exam Priorities Letters. *See, e.g.,* Sidley Update "FINRA Issues Its 2017 Exam Priorities," available at https://www.sidley.com/en/insights/newsupdates/2017/01/finra-issues-its-2017-exam-priorities.

specifically highlights cybersecurity-related procedures that require regular risk assessments and detailed testing to resolve high-risk concerns. FINRA also states that the best cybersecurity programs require employees to participate in regular cybersecurity training and testing.

Outside Business Activities and Private Securities Transactions

FINRA rules require registered representatives to notify their firms of proposed outside business activities (OBAs) and all associated persons to notify their firms of proposed private securities transactions (PSTs). In its Report, FINRA notes that individuals often failed to notify their firms of OBAs and PSTs and that certain firms did not have adequate written procedures for reviewing OBAs and PSTs.

Best practices regarding OBAs and PSTs typically involve firms establishing proactive compliance efforts. According to FINRA, part of this proactive approach often includes frequent training of registered representatives and associated persons to keep them aware of their OBA and PST reporting obligations. Some firms periodically required these individuals to complete open-ended questionnaires and attestations while implementing tools to identify and monitor individuals involved in undeclared OBAs and PSTs.

Anti-Money-Laundering (AML) Compliance Program

FINRA requires members to develop and implement a written AML program reasonably designed to comply with the applicable laws and regulations. Some firms failed to establish and implement risk-based policies to handle suspicious transactions or improperly delegated monitoring responsibilities to employees within the firm.

While many firms experienced difficulty in adjusting their AML programs to match their business growth, FINRA states that the best AML programs are appropriately tailored to their firms' size and business model. FINRA observes that firms with the most effective AML programs regularly tested customer accounts to help ensure that the firms collected and verified information related to applicable laws and regulations, as well as to ensure the adequacy of suspicious activity monitoring. In many cases, these firms designed role-specific training programs for all employees participating in their AML programs.

Product Suitability

FINRA rules place obligations on members and associated persons to ensure that investment recommendations are appropriate given a particular individual's investment profile. In its Report, FINRA expresses concern in connection with firms' practices related to unit investment trusts (UITs) and exchange-traded funds (ETFs). FINRA observes that in many instances, firms advised customers to roll over their UITs early without reviewing for suitability. Short-term UIT trading causes investors to incur additional sales charges, and some firms failed to implement adequate internal controls to identify potential sales practice abuse by registered representatives. Similarly, many firms failed to adequately supervise and review recommendations to purchase complex products like leveraged or inverse ETFs.

The most effective product suitability programs included thorough training on the performance and risks of UITs and ETFs. Training typically emphasized the communication of product risks to customers and outlined criteria to consider in determining whether a product was suitable for a specific customer.

Best Execution

According to its Report, FINRA observed best execution deficiencies at firms of all sizes in nearly all classes of securities. These deficiencies included failure to compare execution quality of routed orders against potential executions at competing markets, failure to conduct review of certain order types and failure to perform execution quality reviews in a manner consistent with FINRA rules and available guidance. Regarding effective best execution procedures, FINRA emphasizes in its Report the importance of regular and rigorous reviews for execution quality. FINRA states that firms should establish procedures describing the reviews that must be performed and documentation standards. FINRA states that to assist a regulator in understanding how firms make routing decisions, firms should thoroughly document their rationale and the data or other information that the firm considers in its routing strategies.[2]

Market Access Controls

FINRA observed many types of deficiencies in firms' market access controls. Among these were instances in which firms failed to establish reasonable pre-trade capital and credit thresholds for their market access programs. In addition, FINRA observed numerous instances where firms did not appropriately tailor erroneous order controls to particular products, situations or order types. Occasionally, FINRA also found that instead of establishing their own thresholds, firms allowed outside vendors to set capital thresholds.

Examples of best practices for market access programs from the FINRA Report include maintenance of reasonable documentation to support thresholds, conducting periodic reviews of thresholds and establishing procedures that describe the process to adjust a threshold on an intraday and permanent basis. FINRA also highlights the appropriate use of "hard" blocks to prevent entry of certain orders as opposed to "soft" blocks that merely provide warnings to users with market access.

Additional Observations

FINRA concludes its Report by mentioning additional areas where some firms faced challenges in meeting their compliance obligations. The final section discusses alternative investments held in individual retirement accounts (IRAs), net capital and credit risk investments, order capacity, Regulation SHO, and Trade Reporting and Compliance Engine (TRACE) reporting. Regarding alternative investments held in IRAs, FINRA observed many instances of firms failing to maintain custody of investment assets or keeping incorrect records of customer positions. In seeking to comply with the Securities and Exchange Commission's net capital rule, some firms faced difficulty in assessing creditworthiness of nonconvertible debt or money market instruments held in inventory. Further, firms had trouble entering correct capacity codes (e.g., agency, principal, riskless principal) when reporting off-exchange trades. FINRA also observed weaknesses in firms' compliance with Regulation SHO, notably with respect to firms' locate practices. Finally, firms faced many challenges in reporting sales of fixed-income securities in accordance with TRACE rules — in some cases, firms did not have systems or processes to determine whether a particular security was TRACE-eligible.

[2] We note that FINRA recently sent targeted examination letters to a select group of firms to request information as part of a review of how firms handle conflicts of interest related to order routing.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work or

James Brigagliano
Partner
jbrigagliano@sidley.com
+1 202 736 8135

W. Hardy Callcott
Partner
hcallcott@sidley.com
+1 415 772 7402

Kevin J. Campion
Partner
kcampion@sidley.com
+1 202 736 8084

Michael D. Wolk
Partner
mwolk@sidley.com
+1 202 736 8807

Timothy B. Nagy
Counsel
tnagy@sidley.com
+1 202 736 8054

Andrew J. Sioson
Associate
asioson@sidley.com
+1 202 736 8351

Sidley Securities & Derivatives Enforcement and Regulatory Practice

Sidley's Securities & Derivatives Enforcement and Regulatory group advises and defends clients in a wide range of securities- and derivatives-related matters. With more than 150 lawyers in 10 offices worldwide, we provide comprehensive regulatory, enforcement, and litigation solutions in matters involving the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Financial Industry Regulatory Authority (FINRA), self-regulatory organizations (SROs), state attorneys general and state securities regulators. Our team is distinctive in that it combines the strength of nationally recognized enforcement lawyers with the skills of equally prominent counseling lawyers. We work collaboratively to provide our clients with informed, efficient and effective representation.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.

SIDLEY

BEIJING · BOSTON · BRUSSELS · CENTURY CITY · CHICAGO · DALLAS · GENEVA · HONG KONG · HOUSTON · LONDON · LOS ANGELES · MUNICH · NEW YORK · PALO ALTO · SAN FRANCISCO · SHANGHAI · SINGAPORE · SYDNEY · TOKYO · WASHINGTON, D.C.