2022 SEC and FINRA Examination and Enforcement Priorities

March 28, 2022 | 12:30 - 1:30 p.m.
Fordham Law School
via Zoom Webinar

CLE COURSE MATERIALS
Table of Contents

1. Speaker Biographies
2. CLE Materials

2022 SEC and FINRA Examination and Enforcement Priorities

Panel Discussion


FINRA Publishes 2021 Report on FINRA’s Examination and Risk Monitoring Program. FINRA. (2021)

Venetia Woo. FINRA 2022 Examination and Enforcement Priorities. Accenture. (March 12, 2022)

Six Key Takeaways from the SEC’s Most Recent Proposed Cybersecurity Rules for Registrants. Debevoise & Plimpton. (March 14, 2022)

Four Takeaways from the SEC’s Proposed Cybersecurity Rules. Debevoise & Plimpton. (February 17, 2022)

SEC Cybersecurity Update: Chair Gensler Offers Insight into Upcoming Regulation. Debevoise & Plimpton. (January 26, 2022)

Aaron Mendelsohn. Mandatory ESG Disclosure Rules are Coming. Accenture. (September 28, 2021)

Aaron Mendelsohn. Don’t Ignore the SG in ESG: Why Companies should Focus on Social and Governance as much as on the Environmental Branch. Accenture. (December 7, 2021)
Richard Best  
**Director, New York Regional Office, U.S. Securities and Exchange Commission**

Richard R. Best was named Regional Director of the U.S. Securities and Exchange Commission’s New York Regional Office in September 2020. He was previously the Regional Director of the Salt Lake Regional Office, serving from July 2015 to February 2018, and Regional Director of the Atlanta Regional Office, serving from February 2018 to September 2020.

Before coming to the Commission, Mr. Best was a Chief Counsel in the Department of Enforcement of the Financial Industry Regulatory Authority (FINRA). Mr. Best was also a Director, Senior Trial Attorney and Trial Attorney at FINRA.

Mr. Best previously worked as an Assistant District Attorney in the Office of the Bronx County District Attorney. He was a supervisor in the Office’s Rackets Bureau where he managed high-profile public integrity and organized crime prosecutions, among other matters.

Mr. Best received his bachelor’s degree from the State University of New York, College at Old Westbury, and a law degree from the Howard University School of Law.

Charu Chandrasekhar  
**Counsel, White Collar & Regulatory Defense Group, Debevoise & Plimpton**

Charu A. Chandrasekhar is a litigation counsel based in the New York office and a member of the firm’s White Collar & Regulatory Defense Group. Her practice focuses on securities enforcement and government investigations, internal investigations and complex commercial litigation.

Prior to joining the firm, Ms. Chandrasekhar served as an Assistant Regional Director in the SEC’s Division of Enforcement and as the founding Chief of the Division’s Retail Strategy Task Force. Ms. Chandrasekhar also served as a Senior Advisor and Senior Counsel in the Division of Enforcement’s Market Abuse Unit.

During her eight years at the SEC, Ms. Chandrasekhar successfully investigated and brought numerous high-profile enforcement cases, including multiple matters involving cutting-edge and complex practices across the securities markets and federal securities laws. She supervised and participated in investigations involving insider trading by corporate insiders, broker-dealers, and hedge funds; antifraud and regulatory violations by stock exchanges, alternative trading systems, and other trading venues; investment advisers; cybersecurity and digital assets; and market manipulation. Her notable matters included the Commission’s largest settlement against a dark pool; one of the Commission’s largest stock exchange settlements, which involved the Commission’s first-ever charge under Regulation SCI; charges against an underwriter in connection with one of the largest offering frauds involving an international issuer listed on an American securities exchange; and multiple insider trading cases with parallel criminal matters. In her service at the SEC in two national enforcement groups, Ms. Chandrasekhar routinely investigated and coordinated matters with senior SEC enforcement officials and enforcement staff from the SEC’s Home Office and eleven regional offices.

Ms. Chandrasekhar’s government service included coordination on parallel matters with the United States Department of Justice, the New York Attorney General’s Office, FINRA, and other domestic and international securities regulators. She also consulted routinely on matters involving registered investment advisers and broker-dealers with the New York Regional Office’s Division of Examinations.

Ms. Chandrasekhar received the Chairman’s Award for Main Street Investors for her accomplishments on the Retail Strategy Task Force, as well as several Enforcement Division Director’s Awards for her successful enforcement matters.

Prior to joining government, Ms. Chandrasekhar was a counsel at a major international law firm and clerked for the Honorable Sonia Sotomayor on the U.S. Court of Appeals for the Second Circuit. Ms. Chandrasekhar received her J.D. cum laude in 2004 from Harvard Law School, where she was
Christopher Kelly
Senior Vice President and Deputy Head of Enforcement, Financial Industry Regulatory Authority

Christopher Kelly serves as the Deputy Head of Enforcement at FINRA. In that role, he oversees the work of more than 175 attorneys who work in FINRA’s Enforcement Department.

He joined FINRA in 2014 and served as Chief Counsel in FINRA’s North Region until early 2018. Prior to joining FINRA, Mr. Kelly served as Deputy Chief of the Criminal Division at the U.S. Attorney’s Office for the District of New Jersey. In that role, Mr. Kelly supervised more than 35 Assistant U.S. Attorneys in the Office’s white-collar units: Economic Crimes, National Security, Healthcare and Government Fraud, and Cybercrime. Prior to his promotion to the position of Deputy Chief, Mr. Kelly served as the Chief of the Economic Crimes Unit at the U.S. Attorney’s Office, where he oversaw the Office’s prosecution of complex economic crimes, including crimes involving insider trading, securities fraud, tax evasion, bank fraud, corporate fraud and embezzlement. Mr. Kelly also served as the lead prosecutor on numerous criminal prosecutions. Prior to joining the U.S. Attorney’s Office, he was an associate at the law firm Dechert LLP. Mr. Kelly also clerked for the Honorable Joseph E. Irenas, U.S. District Court Judge for the District of New Jersey.

Mr. Kelly graduated from Duke University and Harvard Law School.

Venetia Woo
Principal Director, Regulatory Strategy & Capital Markets Lead, Accenture

Venetia is a Principal Director and leads the Capital Markets Finance & Risk Regulatory Strategy practices that helps corporates and financial institutions plan the adoption of new and emerging regulations, remediate, and navigate their regulatory relationships. She focuses clients when restructuring businesses or entering new markets, businesses, or products. She also advises agency regulators and boards of directors in discharging their duties in the face of new technologies, asset classes and risks. Additionally, she is Accenture’s Global Libor Advisor and participates in global initiatives such as ARRC’s Outreach and Communication Working group. You can reach Venetia at: venetia.w.woo@accenture.com.

Aaron Mendelsohn
Principal Director, Digital Risk & Compliance, Accenture

Aaron is a Principal Director on Accenture’s Digital Risk & Compliance team. Aaron is a lawyer by training and has 20+ years of financial regulatory and fraud investigations experience in the private and public sectors. Aaron was a Senior Counsel in FINRA’s Enforcement Department and a federal prosecutor at the U.S. Department of Justice, where he investigated and prosecuted economic crimes and securities industry violations. Aaron has also served as an Adjunct Professor of Law at Fordham teaching International Financial Crime. Throughout his career, Aaron has worked on cases with the SEC, CFTC, OCC, PCAOB, FinCEN, and other federal, state, and international regulators and law enforcement agencies.

Aaron received his BA in History and Art History from Middlebury College and his JD from Northwestern Law School. Aaron can be reached at Aaron.Mendelsohn@Accenture.com
2021 EXAMINATION PRIORITIES
Division of Examinations
DISCLAIMER: This statement represents the views of the staff of the Division of Examinations. It is not a rule, regulation, or statement of the U.S. Securities and Exchange Commission (SEC). 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 THE LEADERSHIP TEAM

This year marks the 25th anniversary of the creation of the U.S. Securities and Exchange Commission (SEC) Office of Compliance Inspections and Examinations (OCIE). During that time, we have grown in size and share of the SEC’s workforce to become the second largest office or division at the SEC—with more than 1,000 employees across all 11 regional offices and the Washington, DC, headquarters. Over the past 25 years, our examination responsibilities have substantially increased with the organic growth in the securities markets and industry and with the introduction of many new types of registered firms, all highlighting the growing breadth and complexity of our mission.

To better reflect the important contributions of the examination program and our overall role at the SEC, we are honored and proud that on December 17, 2020, the Commission unanimously supported the decision to rename OCIE the “Division of Examinations.”¹ This significant step recognizes the important role we have, both within the SEC, as well as externally, to promote a strong culture of compliance within the financial services industry.

The Division of Examinations (the Division or EXAMS) is pleased to announce our examination priorities for fiscal year (FY) 2021, marking the 9th 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.

DID YOU KNOW?

On December 17, 2020, the Commission unanimously supported the decision to rename OCIE the “Division of Examinations.”

Global Pandemic: Observations and Impacts

The past year has been unprecedented in the markets, our careers, and our lives. The pandemic has impacted everyone in different, and in some cases profound ways—including health and medical concerns, care for family members, financial stresses, virtual schooling, and social distancing. The year 2020 ushered in many challenges and changes.

There has been change in almost every facet of our lives, including in the delivery of financial services and the operations of the financial services industry. Generally, we observed that the financial markets’ operations and systems continued to work as designed, with exchanges, clearing agencies, investment advisers, broker-dealers, and other market participants adapting to significant remote work and continuing to operate largely without incident. While there certainly were challenges, and we observed adjustments to many processes, particularly those that involved manual processing or were not automated, overall, the delivery of financial services continued in the pandemic environment as it should have and as investors and other market participants have come to rely and depend upon.

Early on in the pandemic, we issued a statement on our own operations noting the shift to correspondence examinations and our outreach efforts to registered firms to assess pandemic-related operational resiliency challenges. The Division pivoted to focus on the most pressing risks—including examining whether registered firms’ business continuity plans were updated, operational and effective, and addressing increased cybersecurity risks facing firms and investors. We published a COVID-19 Risk Alert to share observations from this work and provided observations and recommendations to assist firms’ pandemic response.

---


In addition to the cybersecurity recommendations in the COVID-19 Risk Alert, we published two cyber-specific risk alerts in conjunction with the Division’s heightened focus in this area since the onset of the pandemic. First, our Ransomware Risk Alert highlights the risk and provides observations regarding ransomware attacks, which are when perpetrators typically hack into a victim’s computer system, seizing control and encrypting data, then demand compensation (a ransom) in exchange for maintaining the integrity and/or confidentiality of customer data, or for the return of control over the firm’s systems.\(^4\) Second, our Credential Compromise Risk Alert highlights observations and responses to credential stuffing attacks, which exploit the tendency for people to reuse their passwords across multiple websites and systems, by cyber attackers who obtain lists of previously compromised usernames, email addresses, and corresponding passwords from the dark web in an attempt to log in and gain unauthorized access to a customer account.\(^5\) These risk alerts built on a special report published early in 2020 on Cybersecurity and Resiliency Observations that highlighted the importance of strong cyber-hygiene and protections.\(^6\)

As we look beyond the pandemic, although uncertainties remain, we know that both firms and the Division will continue to adapt, innovate, and work to ensure strong compliance and investor protection.


Regulation Best Interest and Form CRS

This past year saw the implementation of Regulation Best Interest and over 13,000 Form CRS filings. EXAMS, working closely with the SEC’s other divisions and offices, carefully developed new examination approaches to both promote compliance and inspect firms in both our broker-dealer and investment adviser/investment company programs. To do so, we began by communicating our intentions. In April, we issued two risk alerts: Examinations that Focus on Compliance with Regulation Best Interest and Examinations that Focus on Compliance with Form CRS. These risk alerts provided firms and their chief compliance officers (CCOs) with sample request lists and identified key areas we planned to focus on in our initial examinations.

We also communicated our results. In October, after completing many initial examinations, we shared preliminary observations at a Roundtable on Regulation Best Interest and Form CRS. This public roundtable highlighted to firms and CCOs initial observations on Regulation Best Interest and Form CRS implementation. For Regulation Best Interest, we observed that firms generally responded by updating their written supervisory procedures (WSPs) and conducted training. Some firms’ WSPs incorporated specific processes to comply with the requirements of Regulation Best Interest, whereas we noted potential concerns with WSPs that simply restated the standards, but did not provide any meaningful guidance as to how these should be implemented.

For Form CRS, we saw a wide variety of approaches that firms used to comply with the requirements of Form CRS, and generally observed firms complying with the Form’s requirements. Many firms appeared to make effective use of hyperlinks in their digital Form CRSs. We also observed that many firms are generally avoiding legalese and generic boilerplate language, but we also noted the readability of some Form CRSs could still be improved. Some firms did not adequately respond to the Form CRS disciplinary disclosure requirements, an area all firms should ensure they address. In addition, we identified and notified hundreds of firms that they had failed to timely file a Form CRS.

DID YOU KNOW?
EXAMS identified and notified hundreds of firms that they had failed to timely file a Form CRS.

---

In December, staff from the Division issued a Statement on Recent and Upcoming Regulation Best Interest Examinations. The statement identified components of Regulation Best Interest that may be the subject of focus in the next phase of examinations, including how firms have considered costs in making a recommendation and the processes firm personnel have used to recommend complex products.

EXAMS continues to participate in the agency’s Inter-Divisional Standards of Conduct Implementation Committee, and would also like to remind market participants and other members of the public that they are encouraged to send questions to IABDQuestions@sec.gov. In addition, staff FAQs have been issued on Regulation BI (FAQs on Regulation Best Interest) and Form CRS (FAQs on Form CRS).

**Importance of Compliance**

We continue to believe it is important to emphasize that compliance programs, CCOs 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 CCOs with full responsibility, authority, and resources to develop and enforce policies and procedures of the firm. In a November speech, Director Driscoll highlighted his views on what it means to have an empowered CCO in a position of sufficient seniority and with the necessary authority. The speech also addressed firms’ continued need to address compliance, such that it has adequate resources commensurate with the role. And 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.

---

FY2020 Results

The Division of Examinations 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. The Division completed 2,952 examinations in FY2020, which is a 4.4 percent decrease from FY2019. This small decrease, when viewed in light of the impact of the pandemic, is illustrative of the staff’s hard work, resiliency and dedication to the SEC’s and the Division’s mission to protect investors.

The Investment Adviser/Investment Company (IA/IC) Program

The Division of Examinations reports annually the percentage of the population of registered investment advisers (RIAs) examined each year. This metric is important as the Division is the primary, and often only, regulator responsible for examining this segment of our registered firm population. 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 the Division oversees increased from about 12,000 to more than 13,900, and the assets under management of RIAs increased from approximately $67 trillion to $97 trillion.

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 3,900 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 11 percent of RIAs provide advisory services to a mutual fund, exchange-traded fund, or other registered investment company. Despite this significant growth and complexity, the Division 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. These efforts continue to pay dividends: The Division has increased its examination

DID YOU KNOW?

In the last five years, the number of RIAs the Division oversees increased from about 12,000 to more than 13,900, and the assets under management of RIAs increased from approximately $67 trillion to $97 trillion.
coverage of RIAs over the past several years from 10 percent in 2014 to a high of 17 percent in 2018. The Division’s coverage of RIAs in 2020, a year in which the RIA population continued to increase and the pandemic necessitated a mid-year shift to remote examining, was 15 percent.

The Division also prioritizes the examinations of investment company complexes, which will remain a core focus for examinations in FY2021. In FY2020, the Division completed more than 100 examinations of investment company complexes, as well as conducting hundreds of outreach calls to both investment company complexes and RIAs to assess market impacts from the pandemic.

While the Division 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. The Division’s coverage rates will likely not keep pace with the continued growth in the population and complexity, without corresponding staffing increases. While the Division 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 the Division of Examinations.

**Broker-Dealer and Exchange (BDX) Program**

BDX devoted significant time to preparing for the implementation, and conducting its first examinations, of Regulation Best Interest. This involved working in close coordination both within the Commission as well as with the Financial Industry Regulatory Authority (FINRA) to develop examination materials such as toolkits and other resources to provide guidance and extensive training to examination staff. BDX also began preparations for the security-based swap regulations through the development of examination materials and evaluation of necessary data sources. Even with these significant work-streams and the disruptions caused by the pandemic, BDX completed over 330 examinations of broker-dealers, over 110 examinations of national securities exchanges, and over 90 examinations of municipal advisors and transfer agents.
Other Program Areas
The FINRA and Securities Industry Oversight group (FSIO) completed over 150 examinations of FINRA, including inspections of critical FINRA program areas and oversight reviews of FINRA’s examinations. FSIO also held frequent monitoring meetings with FINRA departments to assess the effectiveness of FINRA’s programs, including monitoring FINRA’s exam program transformation and the many adjustments to approaches and operations that were necessary across FINRA due to the pandemic. In addition, FSIO completed examinations and similar monitoring of the Municipal Securities Rulemaking Board (MSRB).

The Clearance and Settlement Examination Program (CS), working with the Technology Controls Program (TCP), completed 28 examinations of clearing agencies, nearly double the number completed in FY2019. TCP completed over 70 examinations in addition to providing technical support to all other program areas within EXAMS as well as to other Commission divisions and offices. Leveraging its expertise in information security, business continuity and incident response, TCP staff supported efforts ranging from responding to account take-overs to contributing to the development of international cybersecurity best practices, and enhancing domestic and international cyber incident response. Finally, while not widely known, the Office of Risk and Strategy (ORS) houses the registrations team, which processed and reviewed over 50,000 filings from registered firms in 2020, including over 13,000 Forms CRS.

Impact of Examinations
Through its work, the Division is promoting compliance and making a difference for investors and our securities markets. For example, during FY2020, the Division 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, the Division 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 FY2020, the Division verified over 4.8 million investor accounts, totaling over $3.4 trillion in assets—an increase of more than 50 percent of investor accounts, and more than twice the value of assets verified in FY2019. Similarly, when RIAs have access to client funds

DID YOU KNOW?
In FY2020, the Division verified over 4.8 million investor accounts, totaling over $3.4 trillion in assets.
or securities, the Division 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, the Division 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.

Another way we promote compliance and protect investors is by encouraging firms to make investors whole when we identify during an examination that fees have been improperly calculated and charged. Examinations closed in FY2020 have so far resulted in firms returning more than $32 million to investors. We may refer certain matters to the Division of Enforcement when findings are significant with respect to such improper charges or other issues.

Many important Enforcement matters have resulted from our Division’s exams and referrals, including, for example: numerous settled matters involving RIAs’ selection of higher cost mutual fund share classes for clients when lower cost options were available; settled actions against advisers for failing to disclose conflicts of interest, fraudulently inflating net asset values and performance results of managed funds, and violating the Custody Rule; settled actions against broker-dealers for net capital deficiencies, violating Regulation SHO, failing to report suspicious activity reports, and failing to supervise registered representatives who made unsuitable recommendations to retail customers; and a settled matter with a large fintech firm who misrepresented that it provided essentially cost free trading and obtained execution equal to or better than its competitors, when in fact customers received inferior execution due, in part, to the firm receiving substantial payment for order flow. More than 130 Enforcement referrals from FY2020 exams were made so far, and we anticipate more to come from our 2020 examinations. Recoveries and referral metrics may lag fiscal year reporting as we continue to work to get results for harmed investors, which, included more than 20 additional referrals in FY2020 from examinations that were completed in FY2019.
Risk, Technology, and Industry Trends

In FY2021, the Division of Examinations will focus on, and respond to, market events and adjust its risk-based examination program as new and emerging risk areas develop. The Division has already had to adjust course this fiscal year to respond to market events. For example, examination staff across the country and across all of the Division’s program areas have, and continue to be, engaged with registrants reviewing and assessing operations, federal securities law compliance, and assessing risk regarding the wide-spread compromise of commonly used network management software and activities around the so called “meme stocks.”

The Division has expanded its ability to respond to new and emerging risk areas with the newly created Event and Emerging Risks Examination Team (EERT). The Division will leverage this new team to proactively engage with registered firms and other market participants about emerging threats and current market events and quickly mobilize to provide expertise and resources to the SEC’s regional offices when critical matters arise. The EERT will help ensure, through examinations and other firm engagement and monitoring activities, firms are better prepared to address exigent threats, incidents, and emerging risks. The EERT will also work with Division staff to provide expertise and support in response to significant market events that could have a systemic impact or that place investor assets at risk. As always, EXAMS will coordinate closely with other SEC divisions and offices, as well as other domestic and foreign regulatory authorities to better assess impact and mitigate burden on firms.

With an increasing number of staff of registered firms working remotely, additional emphasis also will be focused on compliance and operational challenges that may arise, especially in the area of supervision. Prior to the pandemic, firms were already adapting their business models to better meet customer needs, lower costs, look to new revenue streams, and help manage their clients’ overall financial wellbeing. The pandemic may have slowed some of these efforts, but also accelerated other activities. Firms will continue to have a large remote footprint and thus may increasingly utilize new communication technologies, develop new workflows around onboarding customers, as well as expand (and in some cases close) business lines, or offer different products and services. As with any change, certain activities may result in conflicts of interest, which could require new disclosures and mitigation. Newly offered products or strategies could involve new regulatory obligations or necessitate compliance enhancements to systems, including order and portfolio management frameworks. As a result, the Division will carefully evaluate the impact of these types of firm activities.
More globally, we will continue to focus on several key themes and topics. As the financial service industry transitions away from the London Inter-Bank Offered Rate (LIBOR), the Division will continue to engage with firms around their preparedness and related transition activities. EXAMS will also engage with firms to understand the impact to operations, their business activities, and their customers relating to the United Kingdom’s exit from the European Union. Firms should ensure their compliance programs and controls environment continue to adapt and provide strong protections even as business units and offerings change.

EXAMS continues to enhance its use of new technology and advanced data analytics to prioritize examination candidates and further analyze information collected during our inspections. Working with our partners in the Division of Economic and Risk Analysis (DERA), we plan to build upon existing work in predictive modeling and text-based analytics to improve our examination processes and identify risks and outlier activities correlated with compliance and control risks.

While balancing the importance of data protection with effectively protecting investors, the Division has experienced challenges examining non-U.S. based registered firms that are increasingly subject to laws on data protection and privacy, among others, that may impact the cross-border transfers of certain information to the SEC. These challenges are particularly acute with the growing population of offshore RIAs that now number over 900 RIAs, managing nearly $12 trillion in investor assets. Under U.S. securities laws and implementing rules, RIAs are required to provide their records to SEC staff for inspection, and must certify as to this ability to comply on Form ADV. As a result, the Division in conjunction with the Office of International Affairs has been seeking additional information regarding laws that may impact the cross-border transfer of records from offshore registered firms to the SEC through various channels in order to determine whether they can comply with these inspection requirements. Notably, the United Kingdom’s data protection authority has provided guidance that SEC-registered firms based in the United Kingdom can rely on the public interest derogation under the local data protections law to transfer records containing personal data to SEC staff during examinations. We continue to work with both industry and our counterparts in other countries to address these challenges.
Firm and Investor Outreach and Risk Alerts

The Division of Examinations priorities provide an overview of key areas where it intends to focus its resources. That said, the stated priorities and other examinations the Division conducts do not encompass all of our efforts to improve compliance. To promote compliance, and to further the effective and efficient allocation of examination resources, the Division proactively engages with registered firms through outreach events, including national and regional compliance seminars. In FY2020, EXAMS staff participated in or held more than 300 such outreach events, including specific efforts directed toward teachers, vulnerable adults and seniors, and members of the military.

The Division also engaged with and informed the industry through publications designed to raise awareness of compliance and industry risks. During FY2020, the Division published a report on Cybersecurity and Resiliency Observations and eight risk alerts. The risk alerts include:

- Top Compliance Topics Observed in Examinations of Investment Companies and Observations from Money Market Fund and Target Date Fund Initiatives
- Examinations that Focus on Compliance with Form CRS
- Examinations that Focus on Compliance with Regulation Best Interest
- Examination Initiative: LIBOR Transition Preparedness
- Observations from Examinations of Investment Advisers Managing Private Funds
- Cybersecurity: Ransomware Alert
- Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers
- Cybersecurity: Safeguarding Client Accounts against Credential Compromise

The Division will continue its publication of risk alerts that both describe its national initiatives as well as outline findings and observations 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.

DID YOU KNOW?
In FY2020, EXAMS staff participated in or held more than three hundred outreach events, including specific efforts directed toward teachers, vulnerable adults and seniors, and members of the military.

14 All Division of Examinations Risk Alerts are available at: https://www.sec.gov/exams.
Informing Policy

In addition to our other work, we wanted to take a moment to discuss our important role in informing policy. This function represents a significant amount of important internal work that is not always visible, or obvious in our reported metrics. Although the Division of Examinations itself does not create policy, nearly all our work helps to inform, support, and shape policy discussions and decisions made throughout the Commission. This year, our Division’s ability to inform others was never more evident, and never more important. We are immensely proud of the Division’s performance during the market events this past spring, which was particularly noteworthy in light of the pandemic’s impact. The Division used its expertise, experience, process, and initiative to respond to the events and to serve investors. During that time, the Division provided others within the Commission as well as other regulators, real-time updates of registered firms and market participant information on an expedited basis to provide the Commission at large with a robust view of the situation at the time.

Our ability to inform policy is driven by the knowledge that the Division gains from both the thousands of examinations it does each year, and the feedback we receive from other engagements. We collect observations from examinations, track certain risk themes within those exams, work on targeted national and local subject matter initiatives, including recent examples of inquiries focused on environmental, social, and governance investing, LIBOR transition, and pandemic-related business continuity planning assessments to over 800 firms, and accept feedback from countless engagements with registered firms, self-regulatory organizations, other regulators and market participants. Based on this large, robust, and strategic set of data points EXAMS thoughtfully cultivates and analyzes, we are uniquely able to provide the Commission and other SEC divisions and offices with current insight and valuable feedback about the practical aspects of the Commission’s regulatory mandates and the real-world impacts of regulation.

The Division then uses its observations to inform others throughout the Commission. One of the most significant ways is in rulemaking. EXAMS’ input is routinely provided to the SEC’s rulemaking divisions and offices as they consider whether to amend current rules, draft new ones, or provide guidance. In fact, the Division of Examinations has contributed to more than 30 recent rulemakings related to the registrants that we examine.
The Division of Examinations also shares its highly technical and programmatic knowledge to inform areas beyond rulemaking. For example, TCP not only provides technical expertise to the exam staff, but also informs others throughout the Commission on the ever-increasing cybersecurity issues that firms face, and provides critical analyses of the technology-related tips, complaints and referrals the Commission receives. Similarly, our BDX program informs views of other Divisions’ evaluation of requests by registered firms for transaction approvals, and CS uses clearing data to inform others of potential financial stress on firms, which was particularly critical during spring 2020. Likewise, ORS routinely informs policy by sharing information on risks and emerging issues it identifies, including through its Office of Large Firm Monitoring, which holds recurring and ad hoc engagements with some of the largest financial firms in the country. These efforts provided incredibly valuable information and insight to the Commission as it assessed and responded to market events through the pandemic.

The Division of Examinations is a Resource

Finally, please know that the Division of Examinations 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. The Division’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. Thank you for doing your part to protect investors and promote compliance.
THE DIVISION OF EXAMINATIONS FY2021
EXAMINATION PRIORITIES
INTRODUCTION

During FY2021, the Division of Examinations (the Division or EXAMS) will continue to prioritize the examination of certain practices, products, and services that it believes present 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 discussed below are perennial risk areas the Division routinely covers in its examinations. Their importance to investors, the seriousness and frequency of prior years’ examination findings, or both, demonstrate the need for the Division, and registrants, to continue to be vigilant in these significant areas, including continued consideration of environmental, social, and governance (ESG) matters in light of market developments and increasing awareness in this space. The Division will also prioritize emerging risks, including those relating to climate and ESG that are described more fully below. Moreover, these priorities are not exhaustive and will not be the only issues we address in our examinations, published risk alerts, and investor and industry outreach.

While the priorities drive many of the Division’s examinations, we select firms for examination and the areas of focus covered during examinations according to a risk-based analysis, which varies depending on the type of firm and its business activities. For registered investment advisers (RIAs) and broker-dealers, the Division considers dozens of risk factors, which include: products and services offered, including certain products identified as having higher risk characteristics; compensation and funding arrangements; disclosures and representations made to customers; prior examination observations and regulatory history; whether the firm has never been examined, is newly registered, or has not been examined in many years; material changes in firm leadership or other key 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 the Division considers in its risk-based analysis.
Our analytic efforts and examinations remain firmly grounded in the Division’s four pillars: promoting compliance, preventing fraud, identifying and monitoring risk, and informing policy. The Division’s risk-based approach, both in selecting registrants as examination candidates and in scoping risk areas to examine, allows the Division to be flexible and capable of covering emerging and exigent risks to investors and the marketplace as they arise. For example, since March 2020, the Division has actively engaged in ongoing dialogue and outreach efforts with many registrants to assess the impacts of the pandemic on their businesses, employees, and customers. Additionally, the Division has gathered information about, among other things, challenges with operational resiliency and the implementation and effectiveness of registrants’ business continuity plans. The Division undertook these efforts in the interests of protecting investors and the integrity of the markets, which helped inform observations in a published risk alert relating to Select COVID-19 Compliance Risks and Considerations for Broker-Dealers and Investment Advisers.\textsuperscript{15} Finally, to improve our ability to respond to emerging and exigent risks, the Division established the Event and Emerging Risks Examination Team (EERT), which has recently become operational.\textsuperscript{16}

\textbf{DID YOU KNOW?}
To improve our ability to respond to emerging and exigent risks, the Division established the Event and Emerging Risks Examination Team (EERT), which began operating this year.


RETAIL INVESTORS, INCLUDING SENIORS AND INDIVIDUALS SAVING FOR RETIREMENT

The Division will again emphasize the protection of retail investors, particularly seniors and individuals saving for retirement. EXAMS’ two largest program areas—Investment Adviser/Investment Company (IA/IC) and Broker-Dealer and Exchange (BDX)—will continue to prioritize examinations of RIAs, broker-dealers, and dually-registered or affiliated firms, as more and more individuals rely on these financial intermediaries to gain access to the financial markets. EXAMS will focus on investments and services marketed to retail investors, such as mutual funds and exchange-traded products, municipal securities and other fixed income instruments, and microcap securities, such as those traded over-the-counter.

Standards of Conduct

The Commission’s June 2019 adoption of Regulation Best Interest, the Form CRS Relationship Summary (Form CRS), and the Interpretation Regarding Standard of Conduct for Investment Advisers will have a direct impact on the retail investor experience with broker-dealers and RIAs.17

Regulation Best Interest

Regulation Best Interest established a new standard of conduct for broker-dealers and associated persons of a broker-dealer. Regulation Best Interest requires broker-dealers and natural persons who are associated persons of a broker or dealer 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. This general obligation is satisfied only if a broker-dealer complies with four component obligations: a Disclosure Obligation, a Care Obligation, a Conflict of Interest Obligation, and a Compliance Obligation. The standard of conduct draws from

DID YOU KNOW?

Regulation Best Interest established a new standard of conduct for broker-dealers and associated persons of a broker-dealer.

---

key fiduciary principles and cannot be satisfied through disclosure alone. The Division will prioritize examinations to assess compliance with Regulation Best Interest.18 Initial examinations previously undertaken focused on the processes broker-dealers relied on to implement Regulation Best Interest.

In 2021, the Division will expand the scope of examinations to focus on assessing whether broker-dealers are making recommendations that they have a reasonable basis to believe are in customers’ best interests and evaluating broker-dealer processes for compliance and alterations made to product offerings. The Division will also conduct enhanced transaction testing as part of these examinations, and will evaluate firm policies and procedures designed to meet additional elements of Regulation Best Interest, the recommendation of rollovers and alternatives considered, complex product recommendations, assessment of costs and reasonably available alternatives, how sales-based fees paid to broker-dealers and representatives impact recommendations, and policies and procedures regarding how broker-dealers identify and address conflicts of interest.

**RIA Fiduciary Duty**

The Interpretation Regarding Standard of Conduct for RIAs reaffirms, and in some cases clarifies, aspects of an RIA’s fiduciary duty that comprises duties of care and loyalty to its clients. The Division will continue to examine RIAs to assess whether, as fiduciaries, they have fulfilled their duty of care and duty of loyalty. This will include assessing, among other things, whether RIAs provide advice, including whether account or program types continue to be, in the best interests of their clients, based on their clients’ objectives, and eliminate or make full and fair disclosure of all conflicts of interest which might incline RIAs—consciously or unconsciously—to render advice which is not disinterested such that their clients can provide informed consent to the conflict. The Division will continue to focus on risks associated with fees and expenses, complex products, best execution, and undisclosed or inadequately disclosed, compensation arrangements.

---

Form CRS

Form CRS and its related rules require broker-dealers and RIAs to deliver to retail investors a brief customer or client relationship summary that provides information about the firm. Firms must also file their relationship summaries (and any amendments) with the Commission, using the Web Central Registration Depository or Investment Adviser Registration Depository, as applicable, and post the current relationship summary on the firm’s public website, if the firm has one. The Division will prioritize examinations of broker-dealers and RIAs to assess compliance with Form CRS.¹⁹

Fraud, Sales Practices, and Conflicts

It is critically important that broker-dealers, investment companies, and RIAs 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. Conflicts of interest, particularly those with the prospect of financial gain, can improperly influence a firm’s fundamental obligation to act in investors’ best interest. Recent market volatility and industry pressures have impacted fees and other revenues collected by firms. These conditions may cause increased financial stress on firms and their personnel, which may, in turn, lead to increased instances of fraudulent conduct.

Against the backdrop of the standards of conduct described above, examinations will focus on the appropriateness of recommendations and advice provided to retail investors, with a particular emphasis on: (1) seniors, including recommendations and advice made by entities and individuals targeting retirement communities; (2) teachers; (3) military personnel; and (4) individuals saving for retirement.

Additionally, the Division will concentrate on recommendations regarding account type, conversions, and rollovers, as well as the sales practices used by firms for various product types, such as structured products, exchange-traded products, real estate investment trusts, private placements, annuities, digital assets, municipal and other fixed income securities, and microcap securities. In addition to the recommendation of complex products, the Division will examine broker-dealers to assess whether they are meeting their legal and compliance obligations when providing retail customers access to complex strategies, such as options trading, and complex products. The Division will also focus on how firms are complying with the recent changes to the definition of accredited investor when recommending and selling certain private offerings.

¹⁹ See OCIE Risk Alert, Examinations that Focus on Compliance with Form CRS (April 7, 2020) available at https://www.sec.gov/files/Risk%20Alert%20-%20Form%20CRS.pdf.
The Division’s examinations will review firms’ disclosures regarding their conflicts of interest, including those related to fees and expenses. 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 personnel for executing client transactions. One particular area the Division will prioritize is the examination of RIAs operating and utilizing turnkey asset management platforms. Such platforms provide RIAs with technology, investment research, portfolio management and other outsourcing services, and the Division’s examinations will seek to assess whether such fees and revenue sharing arrangements are adequately disclosed.

In addition, concerns may arise when an RIA does not aggregate certain accounts for purposes of calculating fee discounts in accordance with its disclosures. In reviewing fees and expenses, the staff will review for: (1) advisory fee calculation errors, including, but not limited to, failure to exclude certain holdings from management fee calculations; (2) inaccurate calculations of tiered fees, including failure to provide breakpoints and aggregate household accounts; and (3) failures to refund prepaid fees for terminated accounts.

**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 the significant amount or concentration of assets retail investors have invested in a product. The Division will continue to prioritize examinations of issues regarding these products given their importance to retail investors.

**Mutual Funds and Exchange-Traded Funds (ETFs)**

Mutual funds and ETFs are the primary investment vehicle for many retail investors. In addition to the other registered investment company priorities identified below, the Division will focus on financial intermediaries’ recommendations and disclosures involving ETFs, including adequacy of risk disclosure, and suitability, particularly in niche or leveraged/inverse ETFs. The Division will also continue to prioritize the examination of incentives provided to financial services firms and professionals that may influence the selection of particular higher cost mutual fund share classes when lower cost classes are available.
Municipal Securities and Other Fixed Income Securities
The importance of timely and accurate municipal issuer disclosure has become even greater as a result of the potentially significant effects of the pandemic on the finances and operations of many municipal issuers. The Division will examine the activities of broker-dealers, underwriters, and municipal advisors to assess whether these firms are meeting their respective obligations, as and to the extent applicable, in relation to municipal issuer disclosure. In addition, the Division 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 disclosures relating to mark-ups and mark-downs.

Microcap Securities
The Division remains committed to deterring microcap fraud, or fraud in connection with securities of companies with a market capitalization under $250 million. During the pandemic, several issuers of microcap securities made questionable claims regarding testing, treatments, and vaccines, among other things. The Commission suspended trading in certain securities, including certain microcap securities, due to concerns about the adequacy and accuracy of information in the marketplace about the issuers. The Division will continue to prioritize examinations of broker-dealers and transfer agents for compliance with their obligations in the offer, sale, and distribution of microcap securities. Focus areas for examinations will include: transfer agent handling of microcap distributions and share transfers; broker-dealer sales practices and their consistency with Regulation Best Interest; and broker-dealer compliance with certain regulatory requirements, including the locate requirement of Regulation SHO, penny stock disclosures under Rules 15g-2 through 15g-6 of the Securities Exchange Act of 1934, and the obligation to monitor for and report suspicious activity and other anti-money laundering (AML) obligations.
INFORMATION SECURITY AND OPERATIONAL RESILIENCY

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. The Division is acutely focused on working with firms to identify and address information security risks, including cyber-attack related risks, and encourages market participants to actively and effectively engage regulators and law enforcement in this effort.

Over the past year, the increase in remote operations in response to the pandemic has increased concerns about, among other things, endpoint security, data loss, remote access, use of third-party communication systems, and vendor management. The Division will review whether firms have taken appropriate measures to: (1) safeguard customer accounts and prevent account intrusions, including verifying an investor’s identity to prevent unauthorized account access; (2) oversee vendors and service providers; (3) address malicious email activities, such as phishing or account intrusions; (4) respond to incidents, including those related to ransomware attacks; and (5) manage operational risk as a result of dispersed employees in a work-from-home environment. In particular, EXAMS will also focus on controls surrounding online and mobile application access to investor account information, the controls surrounding the electronic storage of books and records and personally identifiable information maintained with third-party cloud service providers, and firms’ policies and procedures to protect investor records and information.
In light of substantial disruptions to normal business operations in the past year, the Division will again be reviewing registrants’ business continuity and disaster recovery plans. Building on the efforts noted above concerning our business continuity plan outreach related to the pandemic, the Division will shift its focus to whether such plans, particularly those of systemically important registrants, account for the growing physical and other relevant risks associated with climate change. The scope of these examinations will be similar to the post-Hurricane Sandy work of the Division and other regulators, with a heightened focus on the maturation and improvements to these plans over the intervening years. As climate-related events become more frequent and more intense, we will review whether systemically important registrants are considering effective practices to help improve responses to large-scale events.

FINANCIAL TECHNOLOGY (FINTECH) AND INNOVATION, INCLUDING DIGITAL ASSETS

Innovations in financial technology and capital formation continue at a rapid pace. This transformation has dramatically changed the way firms interact with their customers and clients. The Division remains committed to staying informed about how these developments impact registrants and investors. Some firms (new and existing) are providing financial services to clients or customers in innovative and evolving ways, such as firms providing advice to clients through automated investment tools and platforms (often referred to as “robo-advisers”) or firms offering automated asset allocation, fractional share purchases, customized portfolios, and mobile applications. Among other areas, examinations will focus on evaluating whether firms are operating consistently with their representations, whether firms are handling customer orders in accordance with customer instructions, and review compliance around trade recommendations made in mobile applications.

The use of technology to facilitate compliance with regulatory requirements (RegTech) has experienced immense growth in recent years. RegTech, when implemented appropriately, may increase the efficiency of compliance staff, reduce manual processes, and exponentially increase transaction review capabilities. However, misused or improperly configured RegTech may lead to compliance program deficiencies. Examinations will focus on the implementation and integration of RegTech in firms’ compliance programs.

Alternative data, or data gleaned from non-traditional sources, is increasingly being used by firms, including advisers to private funds and registered investment companies, as part of their business and investment decision-making processes. Reviews will include examining whether firms are implementing appropriate controls and compliance around the creation, receipt, and use of such information.

The digital asset market continues to evolve, and so too does the adoption of distributed ledger technology in financial services and market infrastructure. Examinations of market participants engaged with digital assets will continue to assess the following: (1) whether investments are in the best interests of investors; (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 representatives’ outside business activities.
ANTI-MONEY LAUNDERING

The Bank Secrecy Act requires financial institutions, including broker-dealers and registered investment companies, to establish AML programs that are tailored to address the risks associated with the firm’s location, size, and activities, including the type of products and services offered to customers or investors, and the means by which those products and services are offered. 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 Suspicious Activity Reports (SARs) with the Financial Crimes Enforcement Network (FinCEN). SARs are used to detect and combat terrorist financing, public corruption, market manipulation, and a variety of other fraudulent behaviors.

Given the importance of these requirements, the Division will continue to prioritize examinations of broker-dealers and registered 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 evaluate whether broker-dealers and registered investment companies have adequate policies and procedures in place that are reasonably designed to identify suspicious activity and illegal money-laundering activities.

THE LONDON INTER-BANK OFFERED RATE (LIBOR) TRANSITION

The discontinuation of LIBOR could have a significant impact on the financial markets and may present a material risk for certain market participants, including RIAs, broker-dealers, investment companies, municipal advisors, transfer agents and clearing agencies. Preparation for the transition away from LIBOR is essential for minimizing any potential adverse effects associated with LIBOR discontinuation. EXAMS intends to engage with registrants through examinations to assess their understanding of any exposure to LIBOR, their preparations for the expected discontinuation of LIBOR and the transition to an alternative reference rate, in connection with registrants’ own financial matters and those of their clients and customers.
ADDITIONAL FOCUS AREAS INVOLVING RIAS AND INVESTMENT COMPANIES

RIA Compliance Programs

EXAMS 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, business continuity plans, and valuation of client assets for consistency and appropriateness of methodology. In evaluating the effectiveness of a compliance program, the Division frequently reviews whether RIAs appear to have sufficient resources to perform core compliance responsibilities.

The Division will continue to review the compliance programs of RIAs, including whether those programs and their policies and procedures are reasonably designed, implemented, and maintained. The Division will continue to prioritize examinations of RIAs that have not been examined for a number of years to focus on whether the compliance programs of RIAs have been appropriately adapted in light of any substantial growth or change in their business models. As part of its risk-based examination approach, the Division will also continue to conduct examinations of RIAs that have never been examined, including new RIAs and RIAs registered for several years that have yet to be examined, with a particular focus on firms’ compliance programs.

DID YOU KNOW?

Due to investor demand, RIAs are increasingly offering investment strategies that focus on sustainability. These strategies may include products and services that are referred to by a variety of terms such as sustainable, socially responsible, impact, and ESG conscious. The Division will focus on products in these areas that are widely available to investors.

Due to investor demand, RIAs are increasingly offering investment strategies that focus on sustainability. These strategies may include products and services that are referred to by a variety of terms such as sustainable, socially responsible, impact, and ESG conscious. The Division will focus on products in these areas that are widely available to investors such as open-end funds and ETFs, as well as those offered to accredited investors such as qualified opportunity funds. The Division will review the consistency and adequacy of the disclosures RIAs and fund complexes provide to clients regarding these strategies, determine whether the firms’ processes and practices match their disclosures, review fund advertising for false or misleading statements, and review proxy voting policies and procedures and votes to assess whether they align with the strategies.

---

In addition, the Division 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 RIAs maintain effective compliance programs to address the risks associated with these business models, including conflicts of interest that arise from certain compensation arrangements and outside business activities, best execution, and prohibited transactions.

**Registered Funds, Including Mutual Funds and ETFs**

During examinations of registered investment companies, EXAMS often reviews funds’ compliance programs and governance practices, with a focus on disclosures to investors, valuation, filings with the Commission, personal trading activities, and contracts and agreements. The Division will review mutual fund filings and reports to funds’ boards for compliance with regulatory requirements and for valuation issues. In focusing on valuation and the resulting impact on fund performance, liquidity and risk-related disclosures, the Division will review for investments in market sectors that experienced, or continue to experience, stress due to the pandemic, such as energy, real estate, or products such as bank loans and high yield corporate and municipal bonds. The Division will also review funds’ and advisers’ disclosures and practices related to securities lending.

The Division will also prioritize examinations of mutual funds or ETFs that have not previously been examined or have not been examined in a number of years, and will generally focus on funds’ compliance programs and financial condition, particularly where funds have instituted advisory fee waivers. In addition, the Division will focus on compliance with exemptive relief, including for the newly created non-transparent actively managed ETFs.

Given the high degree of customization and the diversity of data analytics practices and methodologies, liquidity risk management programs (LRMPs) will be a focus area for the Division. As part of its review of funds’ compliance programs, the Division will focus on mutual funds’ LRMPs to determine whether they are reasonably designed to assess and manage the funds’ liquidity risk. The Division will also review the implementation of required liquidity classifications, particularly in light of the recent stresses in the market due to the pandemic.

Money market funds remain an important part of the registered fund industry to retail and institutional investors for cash management. Given their importance to investors, the Division intends to review money market funds’ compliance with stress-testing requirements, website disclosures and board oversight.
RIAs to Private Funds

Over 36 percent of RIAs manage private funds, which frequently have significant investments from pensions, charities, endowments, and families. EXAMS will continue to focus on advisers to private funds, and will assess compliance risks, including a focus on liquidity and disclosures of investment risks and conflicts of interest.

Specifically, the Division will review for, among other things: preferential treatment of certain investors by advisers to private funds that have experienced issues with liquidity, including imposing gates or suspensions on fund withdrawals; portfolio valuations and the resulting impact on management fees; adequacy of disclosure and compliance with any regulatory requirements of cross trades, principal investments, or distressed sales; and conflicts around liquidity, such as adviser led fund restructurings, including stapled secondary transactions where new investors purchase the interests of existing investors while also agreeing to invest in a new fund.

The Division will also focus on advisers to private funds that have a higher concentration of structured products, such as collateralized loan obligations and mortgage backed securities, to assess whether the funds are at a higher risk for holding non-performing loans and having loans with higher default risk than that disclosed to investors. In addition, the Division will examine advisers to private funds where there may have been material impacts on portfolio companies owned by the private fund (e.g., real estate related investments) due to recent economic conditions.

ADDITIONAL FOCUS AREAS INVOLVING BROKER-DEALERS AND MUNICIPAL ADVISORS

In addition to the areas focusing on Regulation Best Interest, sales practices and retail-targeted investments already discussed, the Division’s broker-dealer examinations will also focus on the safety of customer cash and securities, best execution in light of the effects of evolving commissions and other cost structures, certain types of trading activity, and the operations of alternative trading systems. The Division’s municipal advisor examinations will also focus on the areas described below.

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, and compliance
with requirements for borrowing securities from customers. In light of the COVID-19 pandemic, examiners may also assess broker-dealer funding and liquidity risk management practices to assess whether firms have sufficient liquidity to manage stress events.

**Broker-Dealer Trading Practices**

The Division will continue to examine broker-dealer trading practices. Examinations will focus on broker-dealer compliance with best execution obligations in a zero commission environment and compliance with the recently amended Rule 606 order routing disclosure rules. The Division will continue its prior initiative in the area of payment for order flow and its possible effect on order routing and best execution obligations. Examinations will also focus on market maker compliance with Regulation SHO, including the rules regarding aggregation units and locate requirements. The Division will also examine the operations of certain alternative trading systems for consistency with their disclosures provided in Form ATS-N.

**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. The COVID-19 pandemic has affected the finances and operations of many municipal issuers. Consequently, the importance of timely and accurate municipal disclosure is critical to investors. The Division will examine, in light of the COVID-19 pandemic and its potential impacts on municipal advisors and their clients, how municipal advisors adjusted their practices, if at all. The Division will also examine whether municipal advisors have met their fiduciary duty obligations to municipal entity clients, including but not limited to disclosing and managing conflicts of interest and documentation of the scope of their client engagements. The Division will also examine whether municipal advisors have satisfied their registration, professional qualification, continuing education, and supervision requirements and whether municipal advisors have relied on relief from Form MA annual update filing requirements, or the temporary broker exemptive order permitting certain activities in connection with direct placements of municipal securities.

---


MARKET INFRASTRUCTURE

Clearing Agencies

EXAMS will conduct, as required by law, at least one risk-based exam of each clearing agency designated as systemically important and for which the SEC serves as the supervisory agency. These exams will focus on core risks, processes, and controls and will cover the specific areas required by statute, including assessment of financial and operational risk. The Division will also conduct risk-based examinations of other registered clearing agencies and entities exempt from registration as clearing agencies.

The Standards for Covered Clearing Agencies are rules that require covered clearing agencies to, among other things, have policies and procedures that address maintaining sufficient financial resources, protecting against credit risks, managing member defaults, and managing 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 other regulators. Areas of focus may include compliance, legal, recovery and wind down, margin, back-testing, settlement and operations, liquidity risk management, effect of the LIBOR transition, and cybersecurity and resiliency, among other things.

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

---

24 Title VIII of the Dodd-Frank Act requires the SEC to examine, at least once annually, each registered clearing agency that the Financial Stability Oversight Council has designated as systemically important and for which the SEC serves as the supervisory agency.

25 EXAMS consults with the Federal Reserve Board each year on the scope and methodology of the SEC’s Dodd-Frank examinations, as required by the Dodd-Frank 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.
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. The Division will examine the national securities exchanges to assess whether they are meeting their obligations under the federal securities laws. Examinations will focus on exchange operations to monitor, investigate, and enforce member and listed company compliance with, as applicable, exchange rules and the federal securities laws.

Regulation Systems Compliance and Integrity (SCI)

The Commission adopted Regulation SCI to strengthen the technology infrastructure of the U.S. securities markets. Among other things, Regulation SCI requires designated entities (SCI entities), which include national securities exchanges, registered and certain exempt clearing agencies, the Financial Industry Regulatory Authority (FINRA), the Municipal Securities Rulemaking Board (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.

EXAMS 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 governance, IT asset management, cyber threat management/incident response, business continuity planning, and third-party vendor management, including utilization of cloud services. EXAMS may also review whether SCI entities have taken appropriate action in response to past examination findings.
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.

The Division will continue to examine transfer agents’ core functions: the timely turnaround of items and transfers, recordkeeping and record retention, and safeguarding of funds and securities. In light of the COVID-19 pandemic, transfer agent examinations will also consider a firm’s business continuity and disaster recovery programs, as well as their cybersecurity measures and account takeover precautions. Examination candidates will include those transfer agents that present the greatest possible risks to investors and investment channels (i.e., where/how retail investors are more likely to invest), and will include transfer agents that service microcap or municipal bond issues, use novel technological applications (e.g., blockchain or online crowdfunding portal applications), or engage in significant paying agent activity.
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.

EXAMS 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, EXAMS conducts inspections of FINRA’s major regulatory programs. EXAMS also conducts oversight examinations of FINRA’s examinations of certain broker-dealers and municipal advisors. From its observations during all of these inspections and examinations, EXAMS 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 broker-dealers (including registered 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. EXAMS, along with FINRA and the federal banking regulators, conducts examinations of registered firms to assess compliance with MSRB rules. EXAMS 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 the Division’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 regulators. The Division 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/exams. 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.
Introduction

The 2022 Report on FINRA’s Examination and Risk Monitoring Program (the Report) provides firms with information that may help inform their compliance programs. For each topical area covered, the Report identifies the relevant rule(s), highlights key considerations for member firms’ compliance programs, summarizes noteworthy findings from recent examinations, outlines effective practices that FINRA observed during its oversight, and provides additional resources that may be helpful to member firms in reviewing their supervisory procedures and controls and fulfilling their compliance obligations.

FINRA’s intent is that the Report be an up-to-date, evolving resource or library of information for firms. To that end, the Report builds on the structure and content in the 2021 Report by adding new topics (e.g., Disclosure of Order Routing Information, Funding Portals) denoted NEW FOR 2022 and new material (e.g., new exam findings, effective practices) to existing sections where appropriate. (New material in existing sections is in bold type.) In addition, those general findings that are also particularly relevant for firms in their first year of operation are denoted with a star (★).

As always, FINRA welcomes feedback on how we can improve future publications of this Report. Please contact Steve Polansky, Senior Director, Member Supervision at (202) 728-8331 or by email; or Rory Hatfield, Associate Principal Research Analyst, Member Supervision at (240) 386-5487 or by email.

Selected Highlights

In 2021, considerable industry, and in some cases public, attention was focused on topics that FINRA also addressed through its exam and risk monitoring program. These topics include newer SEC Rules (e.g., Regulation Best Interest (Reg BI), Form CRS, amendments to Rule 606), recent increases in the number and sophistication of cybersecurity threats, and the proliferation of securities trading through mobile apps.

Reg BI and Form CRS

During Reg BI’s and Form CRS’ first full calendar year of implementation in 2021, FINRA expanded the scope of its reviews and testing relative to 2020 to execute a more comprehensive review of firms’ processes, practices and conduct in areas such as establishing and enforcing adequate written supervisory procedures (WSPs); filing, delivering and tracking accurate Forms CRS; making
recommendations that adhere with Reg BI's Care Obligation; identifying and mitigating conflicts of interest; and providing effective training to staff. In this Report, FINRA notes its initial findings from its Reg BI and Form CRS reviews during the past year and will share additional findings at a future date.

CAT
FINRA continues to evaluate member firms that receive or originate orders in National Market System (NMS) stocks, over-the-counter (OTC) equity securities and listed options for compliance with Securities Exchange Act of 1934 (Exchange Act) Rule 613 and the CAT NMS Plan FINRA Rule 6800 Series (Consolidated Audit Trail Compliance Rule) (collectively, CAT Rules). This year’s Report addresses compliance with certain CAT obligations, such as reporting CAT information to the Central Repository and maintaining an effective supervision process (including clock synchronization performed by third-party vendors).

Order Handling, Best Execution and Conflicts of Interest
Assessing firms’ compliance with their best execution obligations under FINRA Rule 5310 (Best Execution and Interpositioning) is one of the cornerstones of FINRA’s oversight activities. This oversight has evolved with changes in firms’ business models, for example the advent of the “zero commission” model.

As noted in last year’s Report, FINRA launched a targeted exam to “evaluate the impact that not charging commissions has or will have on the member firms’ order-routing practices and decisions, and other aspects of member firms’ business.” FINRA will share its findings with member firms at a future date.

In addition, FINRA is focusing on firms’ compliance with Rule 606 of Regulation NMS, which requires broker-dealers to disclose information regarding the handling of their customers’ orders in NMS stocks and listed options. This information provides transparency to customers and can help them: better understand how their firm routes and handles their orders; assess the quality of order handling services provided by their firm; and determine whether their firm is effectively managing potential conflicts of interest that may impact their firm’s routing decisions.

Mobile Apps
Advances in technology and its application continue to reshape the way some firms attract and interact with customers on mobile apps. These innovations can benefit investors in several ways, including increasing their market participation, expanding the types of products available to them and educating them on financial concepts. At the same time, however, these apps raise novel questions and potential concerns, such as whether they encourage retail investors to engage in trading activities and strategies that may not be consistent with their investment goals or risk tolerance, and how the apps’ interface designs could influence investor behavior.

FINRA has identified significant problems with some mobile apps’ communications with customers and firms’ supervision of activity on those apps (particularly controls around account openings). FINRA has also observed mobile apps making use of social media to acquire customers, and recently initiated a targeted exam to assess firms’ practices in this area, including with respect to firms’ management of their obligations related to information collected from those customers and other individuals who may provide data to firms; FINRA will share its findings from this review after its completion.

Special Purpose Acquisition Companies (SPACs)
Another topic that has received significant attention is the increased use of Special Purpose Acquisition Companies (SPACs) to bring companies public. For example, in 2019, approximately 25 percent of initial public offerings were accomplished through SPACs; in the first quarter of 2021, this figure was over 70 percent.
FINRA recognizes how SPACs can provide companies with access to diverse funding mechanisms and allow investors to access new investment opportunities; however, as SPAC activity has increased, so too has FINRA's focus on broker-dealers' compliance with their regulatory obligations in executing SPAC transactions. In October 2021, FINRA launched a targeted exam to explore a range of issues, including how firms manage potential conflicts of interest in SPACs, whether firms are performing adequate due diligence on merger targets and if firms are providing adequate disclosures to customers. At a future date, FINRA will share with member firms its findings from this review.

**Cybersecurity**

Cybersecurity threats are one of the primary risks firms and their customers face. Over the past year, FINRA has continued to observe increases in the number and sophistication of these threats. For example, in 2021, FINRA has alerted firms about phishing campaigns involving fraudulent emails purporting to be from FINRA, as well as new customers opening online brokerage accounts to engage in Automated Clearing House (ACH) “instant funds” abuse. FINRA has issued additional regulatory guidance concerning the increase of bad actors using compromised registered representative or employee email accounts to execute transactions or move money; using customer information to gain unauthorized entry to customers’ email accounts, online brokerage accounts or both (i.e., customer account takeover (ATO) incidents); and using synthetic identities to fraudulently open new accounts. FINRA will continue to assess firms’ programs to protect sensitive customer and firm information, as well as share effective practices firms can employ to protect their customers and themselves. Where appropriate, FINRA will also share information about cybersecurity threats to firms.

**Complex Products**

FINRA will continue to review firms' communications and disclosures made to customers in relation to complex products, and will review customer account activity to assess whether firms' recommendations regarding these products are in the best interest of the retail customer given their investment profile and the potential risks, rewards and costs associated with the recommendation. In addition, in August of last year, FINRA launched a targeted exam to review members' practices and controls related to the opening of options accounts which, in some instances, may be used to engage in complex strategies involving multiple options (such as spreads). FINRA will share its findings from this review at a future date.

**How to Use This Report**

FINRA's Risk Monitoring and Examination Programs evaluate member firms for compliance with relevant obligations and consider specific risks relating to each firm, including those relating to a firm's business model, supervisory control system and prior exam findings, among other considerations. While the topics addressed in this Report are selected for their interest to the largest number of member firms, they may include areas that are not relevant to an individual member firm and omit other areas that are applicable.

FINRA advises each member firm to review the Report and consider incorporating relevant practices into its compliance program in a manner tailored to its activities. The Report is intended to be just one of the tools a member firm can use to help inform the development and operation of its compliance program; it does not represent a complete inventory of regulatory obligations, compliance considerations, examination findings, effective practices or topics that FINRA will examine.

FINRA also reminds member firms to stay apprised of new or amended laws, rules and regulations, and to update their WSPs and compliance programs on an ongoing basis, as new regulatory obligations may be part of future examinations. FINRA encourages member firms to reach out to their designated Risk Monitoring Analyst if they have any questions about the considerations, findings and effective practices described in this Report.
Each area of regulatory obligations is set forth as follows:

- **Regulatory Obligations and Related Considerations** – A brief description of:
  - relevant federal securities laws, regulations and FINRA rules; and
  - questions FINRA may ask or consider when examining your firm for compliance with such obligations.

- **Exam Findings and Effective Practices**
  - Noteworthy findings that FINRA has noted at some—but not all—member firms, including:
    - new findings from recent examinations;
    - findings we highlighted in prior Reports and that we continue to note in recent examinations;
    - in certain sections, topics noted as “Emerging Risks” representing potentially concerning practices that FINRA has observed and which may receive increased scrutiny going forward; and
    - for certain topics—such as Cybersecurity, Liquidity Management and Credit Risk—observations that suggested improvements to a firm’s control environment to address potential weaknesses that elevate risk, but for which there are not specific rule violations.
  - Select effective practices FINRA observed in recent exams, as well as those we noted in prior Exam Findings Reports and which we continue to see, that may help member firms, depending on their business model, evaluate their own programs.

- **Additional Resources** – A list of relevant FINRA Notices, other reports, tools and online resources.

The Report also includes an Appendix that outlines how member firms have used similar FINRA reports (e.g., Exam Findings Reports, Priorities Letters) in their compliance programs.

As a reminder, the Report—like our previous Exam Findings Reports and Priorities Letters—does not create any new legal or regulatory requirements or new interpretations of existing requirements. You should not infer that FINRA requires member firms to implement any specific practices described in this report that extend beyond the requirements of existing federal securities provisions or FINRA rules.
Firm Operations

Anti-Money Laundering

Regulatory Obligations and Related Considerations

Regulatory Obligations:
The Bank Secrecy Act (BSA) and implementing regulations form the foundation for member firms’ Anti-Money Laundering (AML) obligations. (The BSA has been amended several times, including by the USA PATRIOT ACT of 2001 and the Anti-Money Laundering Act of 2020.) The implementing regulations impose a number of requirements on broker-dealers, which include implementing and maintaining both AML programs and Customer Identification Programs (CIPs); filing reports of suspicious activity; verifying the identity of legal entity customers; maintaining procedures for conducting ongoing customer due diligence; establishing due diligence programs to assess the money laundering risk presented by correspondent accounts maintained for foreign financial institutions; and responding to information requests from the Financial Crimes Enforcement Network (FinCEN) within specified timeframes.

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires that members develop and implement a written AML program reasonably designed to comply with the requirements of the BSA and its implementing regulations. FINRA Rule 3310 also requires FINRA member firms to, among other things, establish and implement policies, procedures and internal controls that can be reasonably expected to detect and cause the reporting of suspicious activity; provide for an independent test of the AML program each calendar year (or every two years in some specialized cases); and provide ongoing training for appropriate personnel.

Related Considerations:
- Does your firm's AML program reasonably address your business model, new and existing business lines, products, customers, geographic locations and associated AML risks?
- Has your firm experienced substantial growth or changes to its business? If so, has its AML program reasonably grown and evolved alongside the business?
- Do your firm’s AML procedures recognize that the suspicious activity reporting obligation may apply to any transactions conducted by, at or through the firm, even transactions that do not originate with your firm’s customers?
- Does your firm have appropriately designed AML procedures to identify and respond to known indicators of suspicious activity involving low-priced securities, such as those detailed in FINRA Regulatory Notices 19-18 and 21-03?
- Does your firm's independent AML testing confirm that it maintains and implements reasonably designed procedures for suspicious activity detection and reporting?
- Does your firm collect identifying information and verify the identity of all individuals and entities that would be considered customers under the CIP Rule, and beneficial owners of legal entity customers under the Customer Due Diligence (CDD) Rule?
- If your firm uses automated surveillance systems for suspicious activity monitoring, does your firm review the integrity of its data feeds and assess scenario parameters as needed?
- If your firm introduces customers and activity to a clearing firm, how does your firm coordinate with your clearing firm, including with respect to the filing of Suspicious Activity Reports (SARs)?
Has your firm established and implemented appropriate procedures to: communicate cyber events to its AML department, Compliance department or both; fulfill regulatory obligations, such as the filing of SARs; and inform reviews of potentially impacted customer accounts?

Has your firm reviewed FinCEN’s first government-wide priorities for AML and countering the financing of terrorism (AML/CFT) policy ("AML/CFT Priorities"), and considered how the AML/CFT Priorities will be incorporated into its risk-based AML program?

**Emerging Low-Priced Securities Risk**

FINRA has observed an increase in several types of activity in low-priced securities that could be indicative of fraud schemes—including an increase in such activity through foreign financial institutions (FFIs) that open omnibus accounts at U.S. broker-dealers. Recent trends indicate that FFIs may be “nesting” within omnibus accounts of financial institutions based in jurisdictions that are generally considered to be lower risk, such as Canada or the United Kingdom.

To assist member firms in detecting and preventing these schemes—as well as mitigating the harm they cause to investors and the market—FINRA is sharing some of the signs of potentially illicit trading activity in low-priced securities that it has recently observed, which include:

- trading that coincides with a sudden increase in share price or trading volume, in the absence of legitimate news surrounding the company;
- investors depositing large blocks of shares of low-priced securities originating from convertible debt acquired from the issuer or a third party, immediately selling the shares and then transferring the proceeds out of the account;
- transactions in securities of issuers making questionable claims regarding their products or services related to a recent, major event (e.g., the COVID-19 pandemic) or a new trend (e.g., cryptocurrency or non-fungible tokens (NFTs)) or both; and
- increased trading that overlaps with a surge in relevant promotional activity on social media, investor chat rooms and message boards.

Firms can find additional resources concerning potential warning signs of fraudulent activity:

- FINRA’s [Investor Alerts](https://www.finra.org/investor-alerts) and [Investor Insights](https://www.finra.org/investor-insights) webpages
- [Regulatory Notice 21-03](https://www.finra.org//files/notice/21-03.pdf) (FINRA Urges Firms to Review Their Policies and Procedures Relating to Red Flags of Potential Securities Fraud Involving Low-Priced Securities)
- [Regulatory Notice 19-18](https://www.finra.org/registration-and-disclosure/regulatory-notice-19-18) (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)
- SEC’s [Risk Alert on Compliance Issues Related to Suspicious Activity Monitoring and Reporting at Broker-Dealers](https://www.sec.gov/comments/samp/oca-risks-alarm/oca-risks-alarm-20190329-001.pdf)
Exam Findings and Effective Practices

Exam Findings:

- Inadequate Ongoing Monitoring and Reporting of Suspicious Transactions – Failing to establish and implement an AML program reasonably expected to detect and report suspicious activity in compliance with FINRA Rule 3310(a) by, for example:
  - not using AML reports or systems that accurately and reasonably capture potentially suspicious activity, and are free of data integrity issues;
  - not conducting and accurately documenting AML surveillance reviews;
  - not implementing appropriate risk-based procedures to understand the nature and purpose of customer relationships in order to develop a customer risk profile;
  - not implementing procedures that are reasonably designed to investigate inquiries from clearing firms that concern “red flags” of potentially suspicious activity;
  - not tailoring AML programs to risks presented by products, customers, business lines and transactions (e.g., cash management products, low-priced securities trading) and wire and ACH transfers; and
  - not notifying AML departments of events that involve suspicious transactions (e.g., cybersecurity events, account compromises or takeovers, new account fraud, fraudulent wires and ACH transfers).

- Inadequate AML Independent Tests – Failing to comply with FINRA Rule 3310(c) by conducting AML tests that fail to review key aspects of the AML program, are not performed within the required timeframe, are not completed by persons with the requisite independence or are not completed at all.

- Insufficient Compliance With Certain Requirements of the BSA – Failing to establish a risk-based CIP to verify the identity of each customer in compliance with FINRA Rule 3310(b), failing to verify the identity of the beneficial owners of legal entity customers in compliance with FINRA Rule 3310(f) or failing to conduct due diligence on correspondent accounts of foreign financial institutions in compliance with FINRA Rule 3310(b).
Update on Initial Public Offerings (IPOs) of China-Based Issuers

FINRA has observed that some firms are underwriting IPOs and subsequent trading of issuers based in the People’s Republic of China (China-based issuers), raising concerns that the investors in the IPOs may be serving as nominees for an undisclosed control person or persons. These IPOs are typically smaller in size (i.e., less than $100 million) and listed on the lower qualification tiers of U.S. stock exchanges.

FINRA has observed red flags of potentially manipulative trading associated with how these investors open new accounts and trade these securities after the IPO is completed, including:

- numerous unrelated accounts being opened at the same time, including with similar banking information, physical addresses, email address domains and current employer (which is often associated with the IPO issuer);
- documents investors provide in order to open an account or verify source of funds that may have been altered or could be fictitious;
- wire transfers received into these accounts that exceed the financial wherewithal of the investor as indicated on their new account documents, exceed the value of the shares purchased in the IPO and are either sent from similar banks, or bank accounts that share certain identifying information (e.g., employer of account holder, email domain);
- investor accounts being accessed by a different Internet Protocol (IP) or Media Access Control (MAC) address than is known for the customer, granting log in and trading capabilities to a third party or both;
- multiple orders with substantial similar terms being placed at or around the same time by seemingly unrelated investors in the same security that is indicative of “spoofing” or “layering”; and
- investors engaging in trading activity that does not make economic sense.

Given the potential risks, firms underwriting these IPOs and whose customers trade in these securities after the IPO should carefully evaluate whether they have controls in place necessary to identify and report market manipulation, other abusive trading practices and potential AML concerns. Firms can find additional information regarding the risks associated with China-based issuers in recent statements from the SEC:

- Emerging Market Investments Entail Significant Disclosure, Financial Reporting and Other Risks; Remedies are Limited
- Disclosure Considerations for China-Based Issuers
- [Chairman Gensler’s] Statement on Investor Protection Related to Recent Developments in China

Effective Practices:

- **Risk Assessments** – Conducting an initial, formal written risk assessment and updating it based on the results of AML tests, audits and changes in size or risk profile of the firm (e.g., business lines, products and services, registered representatives and customers).

- **Verifying Customers’ Identities When Establishing Online Accounts** – In meeting their CIP obligations, validating identifying information or documents provided by applicants (e.g., Social Security number (SSN), address, driver’s license), including, for example, through “likeness checks”; asking follow-up questions or requesting additional documents based on information from credit bureaus and credit reporting agencies, or digital identity intelligence (e.g., automobile and home purchases); contracting third-party vendors to provide additional support (e.g., databases to help verify the legitimacy of suspicious information in customers’ applications); limiting automated approval of multiple accounts
by a single customer; reviewing account applications for repetition or commonalities amongst multiple applications; and using technology to detect indicators of automated scripted attacks.⁴

- Delegation and Communication of AML Responsibilities – When AML programs rely on other business units to escalate red flags of suspicious activity, establishing clearly delineated written escalation procedures and recurring cross-department communication with AML and compliance staff.

- Training – In meeting their obligations to provide ongoing AML training for appropriate personnel under FINRA Rule 3310(e), establishing and maintaining AML training programs that are tailored for the respective roles and responsibilities of the AML department, as well as departments that regularly work with AML; that address regulatory and industry developments impacting AML risk or regulatory requirements; and that, where applicable, leverage trends and findings from quality assurance controls.

- Detection and Mitigation of Wire and ACH Fraud – In meeting their obligations to conduct ongoing monitoring to identify and report suspicious transactions under FINRA Rule 3310(f), monitoring outbound money movement requests post-ACH setup and restricting fund transfers in certain situations (e.g., identity theft is detected in an investor's account).⁵

### Additional Resources

- **SEC**
  - Risk Alert: Compliance Issues Related to Suspicious Activity Monitoring and Reporting
  - Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities

- **FinCEN**
  - Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic
  - Advisory on Cyber-Events and Cyber-Enabled Crime
  - Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments
  - Anti-Money Laundering and Countering the Financing of Terrorism National Priorities
  - Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs)

- **FINRA**
  - Anti-Money Laundering (AML) Topic Page, which includes:
    - Anti-Money Laundering (AML) Template for Small Firms
    - Regulatory Notice 21-36 (FINRA Encourages Firms to Consider How to Incorporate the Government-wide Anti-Money Laundering and Countering the Financing of Terrorism Priorities Into Their AML Programs)
    - Regulatory Notice 21-18 (FINRA Shares Practices Firms Use to Protect Customers from Online Account Takeover Attempts)
    - Regulatory Notice 21-03 (FINRA Urges Firms to Review Their Policies and Procedures Relating to Red Flags of Potential Securities Fraud Involving Low-Priced Securities)
    - Regulatory Notice 20-32 (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection with Potential Account Takeovers and New Account Fraud)
    - Regulatory Notice 20-13 (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
    - Regulatory Notice 19-18 (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)
FinCEN National AML/CFT Priorities

As noted in Regulatory Notice 21-36, on June 30, 2021, FinCEN issued the AML/CFT Priorities, which identify and describe the most significant AML/CFT threats currently facing the United States (e.g., cybercrime, domestic and international terrorist financing, securities and investment fraud).

The publication of the AML/CFT Priorities does not create an immediate change in BSA requirements or supervisory expectations for member firms, and FINRA is not currently examining for the incorporation of the AML/CFT Priorities into member firms’ AML programs. Nevertheless, in preparation for any new requirements when the final regulations are effective, broker-dealers may wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based AML programs.

Cybersecurity and Technology Governance

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Rule 30 of the SEC’s Regulation S-P requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members’ operations. In addition to firms’ compliance with SEC regulations, FINRA reminds firms that cybersecurity remains one of the principal operational risks facing broker-dealers and expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

Technology-related problems, such as problems in firms’ change- and problem-management practices or issues related to an increase in trading volumes, can expose firms to operational failures that may compromise firms’ ability to comply with a range of rules and regulations, including FINRA Rules 4370, 3110 (Supervision) and 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

Related Considerations:

Cybersecurity

- What is the firm’s process for continuously assessing cybersecurity and technology risk?
- What kind of governance processes has your firm developed to identify and respond to cybersecurity risks?
- What is the scope of your firm’s Data Loss Prevention program, including encryption controls and scanning of outbound emails to identify sensitive information?
- How does your firm identify and address branch-specific cybersecurity risks?
- What kind of training does your firm conduct on cybersecurity, including phishing?
- What process does your firm have to evaluate your firm’s vendors’ cybersecurity controls?
- What types of penetration (“PEN”) testing, if any, does your firm do to test web-facing systems that allow access to customer information or trading?
- How does your firm monitor for imposter websites that may be impersonating your firm or your registered representatives? How does your firm address imposter websites once they are identified?
- What are your firm’s procedures to communicate cyber events to AML or compliance staff related to meeting regulatory obligations, such as the filing of SARs and informing reviews of potentially impacted customer accounts?
Cybercrime

- FINRA continues to observe fraudsters and other bad actors engaging in cybercrime that increases both fraud risk (e.g., synthetic identity theft, customer account takeovers, illegal transfers of funds, phishing campaigns, imposter websites) and money laundering risk (e.g., laundering illicit proceeds through the financial system).

- Events involving, or enabled by, cybercrime are expected to be reported via SARs. FINRA has also published Regulatory Notice 21-18 (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts), which discusses cybersecurity practices firms may find effective in mitigating risks related to ATOs and funds transfers.

Technology Governance

- What controls does your firm implement to mitigate system capacity performance and integrity issues that may undermine its ability to conduct business and operations, monitor risk or report key information?
- How does your firm document system change requests and approvals?
- What type of testing does your firm perform prior to system or application changes being moved into a production environment and post-implementation?
- What are your firm's procedures for tracking information technology problems and their remediation? Does your firm categorize problems based on their business impact?

Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Risk Assessment Process** – Not having an adequate and ongoing process to assess cyber and IT risks at the firm, including, for example, failing to test implemented controls or conducting PEN testing regularly.

- **Data Loss Prevention Programs** – Not encrypting all confidential data, including a broad range of non-public customer information in addition to Social Security numbers (such as other account profile information) and sensitive firm information.

- **Branch Policies, Controls and Inspections** – Not maintaining branch-level written cybersecurity policies; inventories of branch-level data, software and hardware assets; and branch-level inspection and automated monitoring programs.

- **Training** – Not providing ongoing comprehensive training to registered representatives, other firm personnel, third-party providers and consultants on cybersecurity risks relevant to individuals' roles and responsibilities (e.g., phishing).

- **Vendor Controls** – Not implementing and documenting formal policies and procedures to review prospective and existing vendors' cybersecurity controls and managing the lifecycle of firms' engagement with all vendors (i.e., from onboarding, to ongoing monitoring, through off-boarding, including defining how vendors will dispose of non-public client information).
Emerging Vendor Risk

Due to the recent increase in the number and sophistication of cyberattacks during the COVID-19 pandemic, FINRA reminds firms of their obligations to oversee, monitor and supervise cybersecurity programs and controls provided by third-party vendors.

Firms can find guidance in this area in Regulatory Notice 21-29 (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors) and the Cybersecurity and Infrastructure Security Agency's (CISA) Risk Considerations for Managed Service Provider Customers.

- **Access Management** – Not implementing access controls, including developing a “policy of least privilege” to grant system and data access only when required and removing it when no longer needed; not limiting and tracking individuals with administrator access; and not implementing multi-factor authentication (MFA) for registered representatives, employees, vendors and contractors.

- **Inadequate Change Management Supervision** – Insufficient supervisory oversight for application and technology changes (including upgrades, modifications to or integration of firm or vendor systems), which lead to violations of other regulatory obligations, such as those relating to data integrity, cybersecurity, books and records, and confirmations.

- **Limited Testing and System Capacity** – Order management system, online account access and trading algorithm malfunctions due to a lack of testing for changes or system capacity issues.

**Effective Practices:**

- **Insider Threat and Risk Management** – Collaborating across technology, risk, compliance, fraud and internal investigations/conduct departments to assess key risk areas, monitor access and entitlements, and investigate potential violations of firm rules or policies regarding data access or data accumulation.

- **Incident Response Planning** – Establishing and regularly testing (often using tabletop exercises) a written formal incident response plan that outlines procedures for responding to cybersecurity and information security incidents; and developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents.

- **System Patching** – Implementing timely application of system security patches to critical firm resources (e.g., servers, network routers, desktops, laptops, mobile phones, software systems) to protect non-public client or firm information.

- **Asset Inventory** – Creating and keeping current an inventory of critical information technology assets—including hardware, software and data—as well as corresponding cybersecurity controls.

- **Change Management Processes** – Implementing change management procedures to document, review, prioritize, test, approve, and manage internal and third-party hardware and software changes, as well as system capacity, in order to protect non-public information and firm services.

- **Online System Capacity** – Continuously monitor and test the capacity of current systems, and track average and peak utilization, to anticipate the need for additional resources based on increases in accounts or trading volumes, as well as changes in systems.

- **Customer Account Access** – Requiring customers to use MFA to access their online accounts.
Additional Resources
FINRA’s Cybersecurity Topic Page, including:

- **Regulatory Notice 21-29** (FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors)
- **Regulatory Notice 21-18** (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)
- **Regulatory Notice 20-32** (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud)
- **Regulatory Notice 20-30** (Fraudsters Using Registered Representatives Names to Establish Imposter Websites)
- **Information Notice 03/26/20** (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19))
- **Regulatory Notice 20-13** (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- **Small Firm Cybersecurity Checklist**
- **Core Cybersecurity Controls for Small Firms**
- **Firm Checklist for Compromised Accounts**
- **Customer Information Protection Topic Page**
- **Cross-Market Options Supervision: Potential Intrusions Report Card**
- **Non-FINRA Cybersecurity Resources**

Outside Business Activities and Private Securities Transactions

Regulatory Obligations and Related Considerations

Regulatory Obligations:
FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person) require registered representatives to notify their firms in writing of proposed outside business activities (OBAs), and all associated persons to notify their firms in writing of proposed private securities transactions (PSTs), so firms can determine whether to limit or allow those activities. A firm approving a PST where the associated person has or may receive selling compensation must record and supervise the transaction as if it were executed on behalf of the firm.

Related Considerations:
- What methods does your firm use to identify individuals involved in undisclosed OBAs and PSTs?
- Do your firm’s WSPs explicitly state when notification or pre-approval is required to engage in an OBA or PST?
- Does your firm require associated persons or registered persons to complete and update, as needed, questionnaires and attestations regarding their involvement— or potential involvement—in OBAs and PSTs; and if yes, how often?
Upon receipt of a written notice of proposed OBAs, does your firm consider whether they will interfere with or otherwise compromise the registered person’s responsibilities to the firm and the firm’s customers, be viewed by customers or the public as part of the member’s business or both? Does your firm also determine whether such activities should be treated as a PST (subject to the requirements of FINRA Rule 3280)?

Does your firm have a process in place to update a registered representative’s Form U4 with activities that meet the disclosure requirements of that form?

Does your firm take into account the unique regulatory considerations and characteristics of digital assets when reviewing digital asset OBAs and PSTs?

Does your firm record PSTs for compensation on its books and records, including PSTs involving new or unique products and services?

How does your firm supervise activities that are PSTs, including digital asset PSTs, and document its compliance with the supervisory obligations?

Exam Findings and Effective Practices

Exam Findings:

Incorrect Interpretation of Compensation – Interpreting “compensation” too narrowly (by focusing on only direct compensation, such as salary or commissions, rather than evaluating all direct and indirect financial benefits from PSTs, such as membership interests, receipt of preferred securities and tax benefits); and as a result, erroneously determining that certain activities were not PSTs.

Inadequate Consideration of Need to Supervise – Approving participation in proposed transactions without adequately considering whether the firms need to supervise the transaction as if it were executed on their own behalf.

No Documentation – Not retaining the documentation necessary to demonstrate the firm’s compliance with the supervisory obligations for PSTs and not recording the transactions on the firm’s books and records because certain PSTs were not consistent with the firm’s electronic systems (such as where securities businesses conducted by a registered representative would not be captured in their clearing firm’s feed of purchases and sales activity).

No or Insufficient Notice and Notice Reviews – Registered persons failing to notify their firms in writing of OBAs or PSTs; and WSPs not requiring the review of such notices, or the documentation that such reviews had taken place.

Inadequate Controls – Inadequate controls to confirm adherence to limitations placed on OBAs or PSTs, such as prohibiting registered representatives from soliciting firm clients to participate in an OBA or PST.

No Review and Recordkeeping of Digital Asset Activities – Failing to conduct the required assessment of OBAs that involve digital assets or incorrectly assuming all digital assets are not securities and therefore, not evaluating digital asset activities, including activities performed through affiliates, to determine whether they are more appropriately treated as PSTs; and for certain digital asset or other activities that were deemed to be PSTs for compensation, not supervising such activities or recording such transactions on the firm’s books and records.

Effective Practices:

Questionnaires – Requiring registered representatives and other associated persons to complete upon hire, and periodically thereafter, detailed, open-ended questionnaires with regular attestations regarding their involvement—or potential involvement—in new or previously disclosed OBAs and PSTs (including asking questions relating to any other businesses where they are owners or employees; whether they are raising money for any outside activity; whether they act as “finders” for issuers seeking new investors; and any expected revenues or other payments they receive from any entities other than the member firm, including affiliates).
Due Diligence – Conducting due diligence to learn about all OBAs and PSTs at the time of a registered representative’s initial disclosure to the firm and periodically thereafter, including interviewing the registered representative and thoroughly reviewing:
- social media, professional networking and other publicly available websites, and other sources (such as legal research databases and court records);
- email and other communications;
- documentation supporting the activity (such as organizational documents); and
- OBAs that involve raising capital or directing securities transactions with investment advisers or fund companies in order to identify potential PSTs.

Monitoring – Monitoring significant changes in, or other red flags relating to, registered representatives’ or associated persons’ performance, production levels or lifestyle that may indicate involvement in undisclosed or prohibited OBAs and PSTs (or other business or financial arrangements with their customers, such as borrowing or lending), including conducting regular, periodic background checks and reviews of:
- correspondence (including social media);
- fund movements;
- marketing materials;
- online activities;
- customer complaints; and
- financial records (including bank statements and tax returns).

Affiliate Activities – Considering whether registered representatives’ and other associated persons’ activities with affiliates, especially self-offerings, may implicate FINRA Rules 3270 and 3280.

WSPs – Clearly identifying types of activities or investments that would constitute an OBA or PST subject to disclosure/approval or not, as well as defining selling compensation and in some cases providing FAQs to remind employees of scenarios that they might not otherwise consider to implicate these rules.

Training – Conducting training on OBAs and PSTs during registered person and associated person onboarding and periodically thereafter, including regular reminders of written notice requirements and for registered persons to update their disclosures.

Disciplinary Action – Imposing significant consequences—including heightened supervision, fines or termination—for persons who fail to notify firms in writing of their OBAs and PSTs, or fail to receive approval of their PSTs for compensation.

Digital Asset Checklists – Creating checklists with a list of considerations to confirm whether digital asset activities would be considered OBAs or PSTs (including reviewing private placement memoranda or other materials and analyzing the underlying products and investment vehicle structures).

Additional Resources
- Regulatory Notice 21-25 (FINRA Continues to Encourage Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- Regulatory Notice 18-08 (FINRA Requests Comment on Proposed New Rule Governing Outside Business Activities and Private Securities Transactions)
- Notice to Members 96-33 (NASD Clarifies Rules Governing RRs/IAs)
- Notice to Members 94-44 (Board Approves Clarification on Applicability of Article III, Section 40 of Rules of Fair Practice to Investment Advisory Activities of Registered Representatives)
Books and Records

Regulatory Obligations and Related Considerations

Regulatory Obligations:
Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and the FINRA 4510 Rule Series (Books and Records Requirements) (collectively, Books and Records Rules) require a firm to, among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to its “business as such.”

Additionally, firms must file a Financial Notification when selecting or changing an archival service provider, and are reminded to document the review of correspondence and confirm that individuals are not conducting supervisory reviews of their own correspondence.

Related Considerations:
- What kind of vendors, such as cloud service providers (Cloud Vendors), does your firm use to comply with Books and Records Rules requirements, including storing required records on electronic storage media (ESM)? How does it confirm compliance with the Books and Records Rules, ESM Standards and ESM Notification Requirements?
- Has your firm reviewed its Books and Records Rules policies and procedures to confirm they address all vendors, including Cloud Vendors?
- If your firm emails its clients and customers links to Virtual Data Rooms (VDRs)—online data repositories that secure and distribute confidential information—does the firm retain and store documents embedded in those links once the VDRs are closed?

Exam Findings and Effective Practices

Exam Findings:
- Misinterpreted Obligations – Not performing due diligence to verify vendors’ ability to comply with Books and Records Rules requirements if they use that vendor; or not confirming that service contracts and agreements comply with ESM Notification Requirements because firms did not understand that all required records must comply with the Books and Records Rules, including records stored using Cloud Vendors’ storage services.
- No ESM Notification – Not complying with the ESM Notification Requirements, including obtaining the third-party attestation letters required by Exchange Act Rule 17a-4(f)(3)(vii).

Effective Practices:
- Contract Review – Reviewing vendors’ contracts and agreements to assess whether firms will be able to comply with the Books and Records Rules, ESM Standards and ESM Notification Requirements.
- Testing and Verification – Testing all vendors’—including Cloud Vendors’—capabilities to fulfill regulatory obligations by, for example, simulating a regulator’s examinations by requesting records and engaging regulatory or compliance consultants to confirm compliance with the Books and Records Rules, ESM Standards and ESM Notification Requirements (and in some cases engaging the consultant to provide the third-party attestation).
- Attestation Verification – Confirming with vendors, including Cloud Vendors, whether the vendors will provide the third-party attestation.
Direct Mutual Fund Business Risk

FINRA observed that some firms did not adequately supervise their direct mutual fund business (i.e., selling mutual fund shares via “check and app” that are held directly by the mutual fund companies) because, for example, they were:

- maintaining blotters that did not include sufficient information to adequately supervise direct mutual fund transactions (e.g., not all transactions are captured or key information is missing, such as customer name, fund symbol and share class);
- miscoding new mutual fund transactions as reinvestments or recurring contributions, which prevented them from going through firms’ surveillance and supervision systems; and
- relying on ad hoc supervisory reviews by an insufficient number of designated principals.

As a result of these arrangements, many firms were unaware of, or had inadequate information about, direct mutual fund transactions that their registered representatives recommended or processed, and were not able to supervise them adequately. In some cases, this inability to supervise direct mutual fund business effectively resulted in firms not being able to identify inappropriate sales charge discounts, unsuitable share class recommendations and short-term mutual fund switching.

As part of their obligations under FINRA Rules 2010 (Standards of Commercial Honor and Principles of Trade), 2110 (Recommendations), 3110 (Supervision) and Reg BI, firms must supervise all activity of their registered representatives related to direct mutual fund transactions. Additionally, Exchange Act Rules 17a-3 and 17a-4 require firms to maintain and keep current purchase and sale blotters that contain relevant information for all direct mutual fund transactions, including redemptions. When evaluating your firm’s supervision of its direct mutual fund business, consider these questions:

- What portion of your firm's mutual fund business is application-based directly with mutual fund companies (in terms of dollar volume and number of accounts)?
- How do your firm’s policies and procedures address supervision of your firm’s direct mutual fund business? What processes (e.g., regularly reviewing exception reports) does your firm use to review direct mutual fund transactions for compliance with applicable FINRA rules and securities regulations? Are such policies and procedures reasonably designed to achieve compliance with applicable securities laws and regulations, and with applicable FINRA rules?
- What information does your firm gather from mutual fund companies or clearing entities (e.g., National Securities Clearing Corporation, Depository Trust and Clearing Corporation) to support its ability to adequately supervise its direct mutual fund business?

For additional guidance, please refer to Regulatory Notice 21-07 (FINRA Provides Guidance on Common Sales Charge Discounts and Waivers for Investment Company Products).
Regulatory Events Reporting

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 4530 (Reporting Requirements) requires firms to promptly report to FINRA, and associated persons to promptly report to firms, specified events, including, for example, violations of securities laws and FINRA rules, certain written customer complaints and certain disciplinary actions taken by the firm. Firms must also report quarterly to FINRA statistical and summary information regarding certain written customer complaints.

Related Considerations:

- Does your firm provide periodic reminders or training on such requirements, and what consequences does your firm impose on those persons who do not comply?
- How does your firm monitor for red flags of unreported written customer complaints and other reportable events?
- How does your firm confirm that it accurately and timely reports to FINRA written customer complaints that associated persons reported to your firm’s compliance department?
- How does your firm determine the problem and product codes it uses for its statistical reporting of written customer complaints to FINRA?

Exam Findings and Effective Practices

Exam Findings:

- No Reporting to the Firm – Associated persons not reporting written customer complaints, judgments concerning securities, commodities- or financial-related civil litigation and other events to the firms’ compliance departments because they were not aware of firm requirements.
- Inadequate Surveillance – Firms not conducting regular email and other surveillance for unreported events.
- No Reporting to FINRA – Failing to report to FINRA written customer complaints that associated persons reported to the firms’ compliance departments.
- Incorrect Rule 4530 Product/Problem Codes – As part of the statistical reporting to FINRA, failing to use codes that correlated to the most prominent product or the most egregious problem alleged in the written customer complaints, but instead reporting less prominent or severe codes or other codes based on the firms’ investigations or other information.

Effective Practices:

- Compliance Questionnaires – Developing detailed annual compliance questionnaires to verify the accuracy of associated persons’ disclosures, including follow-up questions (such as whether they are the subject of any pending lawsuits or have received any written customer complaints).
- Email Surveillance – Conducting email surveillance targeted to identify unreported written customer complaints (by, for example, including complaint-related words in their keyword lexicons, reviewing for unknown email addresses and conducting random email checks).
- Review of Registered Representatives’ Financial Condition – Identifying expenses, settlements and other payments that may indicate unreported events by conducting periodic reviews of their associated persons’ financial condition, including background checks and credit reports.
- Review of Publicly Available Information – Conducting periodic searches of associated persons’ names on web forums, court filings and other publicly available databases, including reviewing for any judgments concerning securities, commodities- or financial-related civil litigation and other reportable events.
Additional Resources

- Regulatory Notice 20-17 (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- Regulatory Notice 20-02 (FINRA Requests Comment on the Effectiveness and Efficiency of Its Reporting Requirements Rule)
- Regulatory Notice 13-08 (FINRA Amends Rule 4530 to Eliminate Duplicative Reporting and Provide the Option to File Required Documents Online Using a New Form)
- FINRA's Rule 4530 Reporting Requirements
- FINRA's Rule 4530 Reporting Codes
- FINRA Report Center – 4530 Disclosure Timeliness Report Card

Firm Short Positions and Fails-to-Receive in Municipal Securities  NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:
As detailed in Regulatory Notice 15-27, customers may receive taxable, substitute interest instead of the tax-exempt interest they were expecting when a firm effects sales to customers of municipal securities that are not under the firm's possession or control. This can occur when firm trading activity inadvertently results in a short position or a firm fails to receive municipal securities it purchases to fulfill a customer's order.

Firms must develop and implement adequate controls and procedures for detecting, resolving and preventing these adverse tax consequences to customers. Such procedures must include closing out fails-to-receive within the time frame prescribed within Municipal Securities Rulemaking Board (MSRB) Rule G-12(h) and confirming that their communications with customers regarding the tax status of paid or accrued interest for municipal securities are neither false nor misleading, in accordance with MSRB Rule G-17.

Related Considerations:
- Does your firm use exception reports to manage its municipal securities' short positions or fails-to-receive? If so, how does your firm use such reports, and which departments are responsible for managing them?
- When municipal securities short positions are identified, does your firm begin to cover the shorts, or do they wait until the trades have settled?
- What is your firm's process to close out fails-to-receive in accordance with the methods and time frame prescribed under MSRB G-12(h)?
- How does your firm detect instances that would require them to pay customers substitute interest? In those circumstances, what is the firm's process for notifying impacted customers and paying them substitute interest in a timely manner? If a customer does not want to receive substitute interest, what alternatives does the firm offer (e.g., offering to cancel the transaction and purchasing a comparable security that would provide tax-exempt interest)?
- How does your firm handle inbound or outbound account transfers sent through the Automated Customer Account Transfer Service (ACAT) that are delivered with no corresponding municipal bonds in possession or control?
Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Controls and Procedures** – Not maintaining adequate procedures and controls for preventing, identifying and resolving adverse consequences to customers when a firm does not maintain possession or control of municipal securities that a customer owns.

- **Inadequate Lottery Systems** – Opting to use a random lottery system to allocate municipal short positions to certain customer accounts, but the system did not fairly or adequately account for or allocate substitute accrued interest payments.

Effective Practices:

- **Preventative Controls** – Maintaining processes to prevent or timely remediate municipal positions from settling short (e.g., covering these positions, finding a suitable alternative, cancelling the customer's purchase).

- **Operational and Supervisory Reports** – Developing operational and supervisory reports to identify customer long positions for which the firm has not taken possession and control of the security.

- **Review of Fail Reports** – Municipal securities principals performing regular, periodic reviews of Fail Reports to comply with the close-out requirements of MSRB Rule G12-(h).

Additional Resource

- *Regulatory Notice 15-27* (Guidance Relating to Firm Short Positions and Fails-to-Receive in Municipal Securities)

**Trusted Contact Persons**  **NEW FOR 2022**

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 4512(a)(1)(F) (Customer Account Information) requires firms, for each of their non-institutional customer accounts, to make a reasonable effort to obtain the name and contact information for a trusted contact person (TCP) age 18 or older. FINRA Rule 4512 also describes the circumstances in which firms and their associated persons are authorized to contact the TCP and disclose information about the customer account.

Related Considerations:

- Has your firm established an adequate supervisory system, including WSPs, related to seeking to obtain and using the names and contact information for TCPs?

- Does your firm educate registered representatives about the importance of collecting and using trusted contact information, where possible?

Exam Findings and Effective Practices

Exam Findings:

- **No Reasonable Attempt to Obtain TCP Information** – Not making a reasonable attempt to obtain the name and contact information of a TCP for all non-institutional customers (e.g., seeking to obtain this information only from senior non-institutional customers, not requesting this information within firm's regularly scheduled 36-month customer account records update letter).
No Written Disclosures – Not providing a written disclosure explaining the circumstances under which the firm may contact a TCP when seeking to obtain TCP information (e.g., when a new non-institutional account is opened or when the firm updates an existing account’s information (in accordance with FINRA Rule 4512(b)).

Effective Practices:

Training – Conducting training, for both front office and back office staff, on the warning signs of potential: (1) customer exploitation; (2) diminished capacity; and (3) fraud perpetrated on the customer.

Emphasizing the Importance of TCP and Promoting Effective Practices –
- Emphasizing at the senior-management level on down the importance of collecting TCP information.
- Using innovative practices, such as creating target goals for collecting TCP and internally publicizing results among branch offices or regions.
- Promoting effective ways of asking for TCP information and seeking feedback from registered representatives and supervisors on techniques that they have successfully used that have not already been publicized across the organization.
- Establishing a system that notifies registered representatives when accessing non-institutional customer accounts that do not have a TCP listed and reminds them to request that information from customers.

Senior Investor Specialists – Establishing specialized groups or appointing individuals to handle situations involving elder abuse or diminished capacity; contact customers’ TCPs—as well as Adult Protective Services, regulators and law enforcement, when necessary—and guiding the development of products and practices focused on senior customers.

Firm Outreach – Hosting conferences or joining industry groups focused on protecting senior customers.

Additional Resources

- SEC’s, NAASA’s and FINRA’s Investor Resources for Establishing a Trusted Contact
- FINRA’s Frequently Asked Questions Regarding FINRA Rules Relating to Financial Exploitation of Senior Investors
- Regulatory Notice 20-34 (Proposed Amendments to FINRA Rule 2165 and Retrospective Rule Review Report)
Emerging Customer Account Information Risks

Effective February 15, 2021, FINRA Rule 3241 (Registered Person Being Named a Customer’s Beneficiary or Holding a Position of Trust for a Customer) requires a registered person to decline being named a beneficiary of a customer’s estate, executor or trustee, or to have a power of attorney for a customer unless certain conditions are met, including providing written notice to the firm and receiving approval. The rule requires the firm with which the registered person is associated, upon receiving required written notice from the registered person, to review and approve or disapprove the registered person assuming such status or acting in such capacity.

Registered persons face potential conflicts of interest when they are named a customer’s beneficiary, executor or trustee, or hold a power of attorney for their customer. These conflicts of interest can take many forms and can include a registered person benefiting from the use of undue and inappropriate influence over important financial decisions to the detriment of a customer.

When assessing your firm’s compliance with Rule 3241, consider these questions:

- Do your firm’s policies and procedures establish criteria for determining whether to approve a registered person assuming either status or acting in either capacity?
- Does your firm perform a reasonable assessment of the risks created by a registered person being named a customer’s beneficiary or holding a position of trust for a customer?
- If your member firm imposes conditions or limitations on its approval, does it reasonably supervise the registered person’s compliance with the corresponding conditions or limitations?
- Does your firm have WSPs, and deliver training, reasonably designed to make registered persons aware of the obligations under the rule and the firm’s related procedures?

Funding Portals and Crowdfunding Offerings  NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Title III of the Jumpstart Our Business Startups (JOBS) Act enacted in 2012 contains provisions relating to securities offered or sold through crowdfunding. The SEC’s Regulation Crowdfunding and FINRA’s corresponding set of Funding Portal Rules set forth the principal requirements that apply to funding portal members.

Funding portals must register with the SEC and become a member of FINRA. Broker-dealers contemplating engaging in the sale of securities in reliance on the crowdfunding exemptions must notify FINRA in accordance with FINRA Rule 4518 (Notification to FINRA in Connection with the JOBS Act).

Related Considerations:

- What steps is your firm taking to confirm all required issuer information, pursuant to Regulation Crowdfunding Rules 201 and 203(a), is publicly available on your firm’s platform?
- Does your firm plan to undergo or has it already undergone an operational or structural change that impacts the capitalization of the firm, pursuant to Funding Portal Rule 110(a)(4)? Has your firm reviewed the membership rules to confirm a Continuing Membership Application (CMA) is not required?
Exam Findings and Effective Practices

Exam Findings:

- **Failure to Obtain Attestation** – Not obtaining the attestation required by Regulation Crowdfunding Rule 404 when using a third-party vendor to store the required records.

- **Missing Disclosures** – Offerings on the platform do not contain all required disclosures as codified in Regulation Crowdfunding, in particular:
  - names of officers and directors of the issuer, and the positions held by these individuals for the past three years;
  - descriptions of the purpose and intended use of proceeds, the process to complete the offering transaction or cancel an investment commitment, the ownership and capital structure, the material terms of any indebtedness of the issuer; and
  - financial statements, as required by Regulation Crowdfunding Rule 201(t).

- **Failure to Report Customer Complaints** – Not reporting written customer complaints, as required by FINRA Funding Portal Rule 300(c).

- **Untimely Required Filings** – Not making required filings in a timely manner—such as filing the funding portal’s Statement of Gross Revenue by the deadline of March 1—and not filing updates or changes to contact information within 30 days of the change.

- **Not Filing CMAs** – Funding portals effecting changes in ownership without obtaining prior approval from FINRA, as required by Funding Portal Rule 110(a)(4).

Effective Practices:

- **Compliance Resources** – Developing annual compliance questionnaires to verify the accuracy of associated persons’ disclosures, including follow-up questions (such as whether they have ever filed for bankruptcy, have any pending lawsuits, are subject to an unsatisfied judgments or liens or received any written customer complaints), as well as compliance checklists and schedules to confirm that required obligations are being met in a timely manner, such as providing all issuer disclosure requirements of Regulation Crowdfunding Rule 201.

- **Supervision** – Implementing supervisory review procedures tailored to funding portal communications requirements that, for example, clearly define permissible and prohibited communications and identify whether any contemplated structural or organizational changes necessitate the filing of a CMA.

Additional Resource

- FINRA’s [Funding Portals Topic Page](#)
Communications and Sales

Reg BI and Form CRS

Regulatory Obligations and Related Considerations

Regulatory Obligations:

The SEC’s Regulation Best Interest (Reg BI) establishes a “best interest” standard of conduct for broker-dealers and associated persons when they make recommendations to retail customers of any securities transaction or investment strategy involving securities, including account recommendations. **Pursuant to this standard, a broker-dealer and its associated persons must not put their financial or other interests ahead of the interests of a retail customer.**

In addition, whether or not they make recommendations, firms that offer services to retail investors must provide them with a Form CRS, a brief relationship summary that discloses material information in plain language (e.g., investment services provided, fees, conflicts of interest, legal and disciplinary history of the firms and financial professionals).

Reg BI and Form CRS became effective on June 30, 2020, and 2021 marked the first full calendar year during which FINRA examined firms’ implementation of related obligations. The findings presented here are thus an initial look at firms’ practices. FINRA will share further findings as we continue to conduct exams and gather additional information on firms’ practices.

Related Considerations:

- **When your firm determines whether it is obligated to comply with Reg BI, does your firm consider the following key definitions in the context of the rule?**
  - “Retail customer” is defined as “a natural person, or the legal representative of such natural person, who:
    - receives a recommendation of any securities transaction or investment strategy involving securities from a broker-dealer; and
    - uses the recommendation primarily for personal, family, or household purposes.”
  - A retail customer “uses” a recommendation of a securities transaction or investment strategy involving securities when, as a result of the recommendation:
    - the retail customer opens a brokerage account with the broker-dealer, regardless of whether the broker-dealer receives compensation;
    - the retail customer has an existing account with the broker-dealer and receives a recommendation from the broker-dealer, regardless of whether the broker-dealer receives or will receive compensation, directly or indirectly, as a result of that recommendation;
    - the broker-dealer receives or will receive compensation, directly or indirectly as a result of that recommendation, even if that retail customer does not have an account at the firm.

- **Do your firm and your associated persons adhere to the Care Obligation of Reg BI when making recommendations by:**
  - exercising reasonable diligence, care and skill to understand the potential risks, rewards and costs associated with a recommendation and having a reasonable basis to believe, based on that understanding, that the recommendation is in the best interest of at least some retail investors;
• considering those risks, rewards and costs in light of the retail customer’s investment profile and having a reasonable basis to believe that a recommendation is in that particular customer's best interest and does not place the broker-dealer’s interest ahead of the customer’s interest; and

• having a reasonable basis to believe that a series of recommended transactions, even if in the retail customer’s best interest when viewed in isolation, is not excessive and is in the retail customer’s best interest when taken together in light of the retail customer’s investment profile?

▶ Do your firm and your associated persons consider costs and reasonably available alternatives when making recommendations to retail customers?

▶ Are your firm’s policies and procedures reasonably designed to identify and disclose or eliminate conflicts, as well as to mitigate conflicts that create an incentive for an associated person of the firm to place his or her interests or the interest of the firm ahead of the retail customer’s interest?

▶ How does your firm test its policies and procedures to determine if they are adequate and performing as expected?

▶ Does your firm place any material limitations on the securities or investment strategies involving securities that may be recommended to a retail customer? If so, does your firm identify and disclose such limitations and prevent those limitations from causing the firm or its associated persons to make recommendations that place the firm's or associated person's interests ahead of the retail customer's interest?

▶ Are your firm’s policies and procedures reasonably designed to identify and eliminate sales contests, sales quotas, bonuses and non-cash compensation that are based on the sale of specific securities or specific types of securities within a limited period of time, or mitigate conflicts for those not required to be eliminated?

▶ Do your firm’s disclosures include a full and fair disclosure of all material facts relating to the scope and terms of the firm’s relationship with retail customers (e.g., material fees and costs associated with transactions or accounts, material limitations involving securities recommendations) and all material facts relating to conflicts of interest that are associated with the recommendation?

▶ What controls does your firm have to assess whether disclosures are provided timely, and if provided electronically, in compliance with the SEC’s electronic delivery guidance?

▶ Do your firm’s policies and procedures address Reg BI, including new obligations that did not exist prior to Reg BI?

▶ Do your firm’s policies and procedures: (1) identify specific individual(s) who are responsible for supervising compliance with Reg BI; (2) specify the supervisory steps and reviews appropriate supervisor(s) should take and their frequency; and (3) note how supervisory reviews should be documented?

▶ If your firm is not dually registered as an investment adviser, commodity trading advisor, municipal advisor or advisor to a special entity, do the firm or any of its associated persons who are not dually registered use “adviser” or “advisor” in their name or title?

▶ Does the firm provide dually-registered associated persons with adequate guidance on how to determine and disclose the capacity in which they are acting?

▶ Has your firm provided adequate Reg BI training to its associated persons, including supervisory staff?

▶ If your firm offers services to retail investors:

• does it deliver Form CRS to each new or prospective customer who is a retail investor before the earliest of: (i) a recommendation of an account type, securities transaction or investment strategy involving securities; (ii) placing an order for the retail investor; or (iii) opening a brokerage account for the investor?
for existing retail investor customers, does the firm deliver Form CRS before or at the time the firm: (i) opens a new account that is different from the retail customer’s existing account; (ii) recommends that the retail customer roll over assets from a retirement account; or (iii) recommends or provides a new service or investment outside of a formal account (e.g., variable annuities or a first-time purchase of a direct-sold mutual fund through a “check and application” process)?

does it file a relationship summary with the SEC through the Central Registration Depository (CRD), if the firm is registered as a broker-dealer; through the Investment Adviser Registration Depository (IARD), if the firm is registered as an investment adviser; or both CRD and IARD, if the firm is a dual-registrant?

does your firm have processes in place to update and file the amended Form CRS within 30 days whenever any information becomes materially inaccurate and to communicate, without charge, any changes in the updated relationship summary to retail investors who are existing customers within 60 days after the updates are required to be made (a total of 90 days to communicate the changes to customers after the information becomes materially inaccurate)?

Exam Findings and Effective Practices

Exam Findings:

Reg BI and Form CRS

WSPs That Are Not Reasonably Designed To Achieve Compliance with Reg BI and Form CRS –

Providing insufficiently precise guidance by:

- not identifying the specific individuals responsible for supervising compliance with Reg BI; and
- stating the rule requirements, but failing to detail how the firm will comply with those requirements (i.e., stating “what” but failing to address “how”).

Failing to modify existing policies and procedures to reflect Reg BI’s requirements by:

- not addressing how costs and reasonably available alternatives should be considered when making recommendations;
- not addressing recommendations of account types;
- not addressing conflicts that create an incentive for associated persons to place their interest ahead of those of their customers; and
- not including provisions to address Reg BI-related recordkeeping obligations and the testing of the firms’ Reg BI and Form CRS policies, procedures and controls.

Failing to develop adequate controls or developing adequate controls but not memorializing these processes in their WSPs.

Inadequate Staff Training – Failing to adequately prepare associated persons to comply with the requirements of Reg BI beyond previous suitability obligations or Form CRS by:

- failing to deliver initial training before the June 30, 2020, compliance date;
- delivering training without making clear Reg BI’s new obligations; or
- delivering training that focused on Reg BI and Form CRS requirements in general, without addressing the specific steps associated persons should take to comply with these requirements.
Failure to Comply With Care Obligation –
- Making recommendations that were not in the best interest of a particular retail customer based on that retail customer's investment profile and the potential risks, rewards and costs associated with the recommendation.
- Recommending a series of transactions that were excessive in light of a retail customer's investment profile and placing the broker-dealer's or associated person's interest ahead of those of retail customers.

Failure to Comply with Conflict of Interest Obligation – Not identifying conflicts or, if identified, not adequately addressing those conflicts.

Improper Use of the Terms “Advisor” or “Adviser” – Associated persons, firms or both, using the terms “advisor” or “adviser” in their titles or firm names, even though they lack the appropriate registration.10

Insufficient Reg BI Disclosures – Not providing retail customers with “full and fair” disclosures of all material facts related to the scope and terms of their relationship with these customers or related to conflicts of interest that are associated with the recommendation, including:
- material fees received as a result of recommendations made (e.g., revenue sharing or other payments received from product providers or issuers, as well as other fees tied to recommendations to rollover qualified accounts);
- potential conflicts of interest (e.g., associated persons trading in the same securities in their personal account(s) or outside employment); and
- material limitations in securities offerings.

Form CRS

Deficient Form CRS Filings – Firms’ Form CRS filings significantly departing from the Form CRS instructions or guidance from the SEC’s FAQ on Form CRS by:
- exceeding prescribed page lengths;
- omitting material facts (e.g., description of services offered; limitations of the firm’s investment services);
- inaccurately representing their financial professionals’ disciplinary histories;
- failing to describe types of compensation and compensation-related conflicts;
- incorrectly stating that the firm does not provide recommendations;
- changing or excluding language required by Form CRS; and
- not resembling a relationship summary, as required by Form CRS.11

Form CRS Not Posted Properly on Website – For firms that have a public website, failing to post or failing to post prominently, in a location and format that is easily accessible to retail investors, the current Form CRS (e.g., requiring multiple click-throughs or using confusing descriptions to navigate to the Form CRS).

Inadequate Form CRS Amendments – Firms not in compliance with Form CRS in relation to material changes because they:
- failed to re-file in CRD in a timely manner (i.e., within 30 days of the date when Form CRS became materially inaccurate); or
failed to communicate or timely communicate changes to existing retail investor customers (e.g., delivering amended summary, with required exhibits, showing revised text or summarizing material changes or communicating the information through another disclosure within 60 days after the updates are required to be made—90 days total from the date when Form CRS became materially inaccurate).

Misconstruing Obligation to File Form CRS –

- Incorrectly determining that filing Form CRS hinges solely on making recommendations, rather than offering services to a retail investor.
- Incorrectly claiming a firm is not subject to the Form CRS delivery obligation because of, among other things, their customer base (e.g., retail investors who are high-net-worth individuals) or the services they offer (e.g., investment company products held directly by an issuer, self-directed accounts)

Effective Practices:

Identifying and Mitigating Conflicts of Interest – Identifying, disclosing, and eliminating or mitigating conflicts of interest across business lines, compensation arrangements, relationships or agreements with affiliates, and activities of their associated persons by:

- establishing and implementing policies and procedures to identify and address conflicts of interest, such as through the use of conflicts committees or other mechanisms or creating conflicts matrices tailored to the specifics of the firm’s business that address, for example, conflicts across business lines and how to eliminate, mitigate or disclose those conflicts;
- sampling recommended transactions to evaluate how costs and reasonably available alternatives were considered;
- providing resources to associated persons making recommendations that account for reasonably available alternatives with comparable performance, risk and return that may be available at a lower cost, such as:
  - worksheets, in paper or electronic form, to compare costs and reasonably available alternatives; or
  - guidance on relevant factors to consider when evaluating reasonably available alternatives to a recommended product (e.g., similar investment types from the issuer; less complex or risky products available at the firm);
- updating client relationship management (CRM) tools that automatically compare recommended products to reasonably available alternatives;
- revising commission schedules within product types to flatten the percentage rate; and
- broadly prohibiting all sales contests.

Limiting High-Risk or Complex Investments for Retail Customers – Mitigating the risk of making recommendations that might not be in a retail customer’s best interest by:

- establishing product review processes to identify and categorize risk and complexity levels for existing and new products;
- limiting high-risk or complex product, transaction or strategy recommendations to specific customer types; and
- applying heightened supervision to recommendations of high-risk or complex products.
Implementing Systems Enhancements for Tracking Delivery of Required Customer Documents
- Tracking and delivering Form CRS and Reg BI-related documents to retail investors and retail customers in a timely manner by:
  - automating tracking mechanisms to determine who received Form CRS and other relevant disclosures; and
  - memorializing delivery of required disclosures at the earliest triggering event.

Implementing New Surveillance Processes – Monitoring associated persons’ compliance with Reg BI by:
- conducting monthly reviews to confirm that their recommendations meet Care Obligation requirements, including system-driven alerts or trend criteria to identify:
  - account type or rollover recommendations that may be inconsistent with a customer’s best interest;
  - excessive trading; and
  - sale of same product(s) to a high number of retail customers;
- monitoring communication channels (e.g., email, social media) to confirm that associated persons who were not investment adviser representatives (IARs) were not using the word “adviser” or “advisor” in their titles; and
- incorporating Reg BI-specific reviews into the branch exam program as part of overall Reg BI compliance efforts, focusing on areas such as documenting Reg BI compliance and following the firms’ Reg BI protocols.

Additional Resources
- FINRA’s SEC Regulation Best Interest Key Topics Page
- SEC's Regulation Best Interest Guidance Page
- SEC's Staff Statement Regarding Form CRS Disclosure
- 2021 FINRA Annual Conference: Regulation Best Interest and Form CRS: Recent Observations and What to Expect Panel
- 2021 Small Firm Virtual Conference: Regulation Best Interest and Form CRS Panel
- You may submit a question by email to IABDQuestions@sec.gov. Additionally, you may contact the SEC's Division of Trading and Markets' Office of Chief Counsel at (202) 551-5777.
Areas of Concern Regarding SPACs

Over the past year, FINRA's review of firms participating in SPAC offerings has focused on the following.

**Due Diligence** – When firms and associated persons act as underwriter, qualified independent underwriter or syndicate member for a SPAC offering, the due diligence conducted at the IPO and merger stages, including as to the relevant officers, directors and control persons of the SPAC and SPAC-sponsor(s) and pre-identified acquisition targets.

**Reg BI** – Written policies and procedures or guidance on recommendations to retail customers, and supervisory systems designed to identify and address conflicts of interest presented by the involvement of the firm, their associated persons or both.

**Disclosure** – Firms' supervision of associated persons who hold positions with, advise or personally invest in SPACs or SPAC sponsors, and whether the associated persons are disclosing their involvement if required by FINRA rules governing OBAs, PSTs and Form U4 amendments.

**Net Capital** – In firm-commitment underwritings, whether firms are correctly taking net capital charges relative to the size of their commitment or using a written agreement with another syndicate member (i.e., “backstop provider”).

**WSPs and Supervisory Controls** – whether firms are maintaining and regularly updating their WSPs and supervisory controls to address risks related to SPACs (e.g., Reg BI, due diligence, information barrier policies, conflicts of interest).

In October 2021, FINRA initiated a targeted review to explore the above areas and other issues relating to SPACs. Additional review areas include training; the use of qualified independent underwriters; underwriting compensation; services provided to SPACs, their sponsors or affiliated entities; and potential merger targets. It is anticipated that, at a future date, FINRA will share with member firms its findings from this review.

Communications with the Public

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 2210 (Communications with the Public) defines all communications into three categories—correspondence, retail communications or institutional communications—and sets principles-based content standards that are designed to apply to ongoing developments in communications technology and practices.

**New member firms are required to file retail communications with FINRA's Advertising Regulation Department during their first year of membership.**

FINRA Rule 2220 (Options Communications) governs members’ communications with the public concerning options. Additionally, MSRB Rule G-21 (Advertising by Brokers, Dealers or Municipal Securities Dealers) contains similar content standards relating to municipal securities or concerning the facilities, services or skills of any municipal dealer.
Related Considerations:

▶ **General Standards –**
  - Do your firm's communications contain false, misleading or promissory statements or claims?
  - Do your firm's communications include material information necessary to make them fair, balanced and not misleading? For example, if a communication promotes the benefits of a high-risk or illiquid security, does it explain the associated risks?
  - Do your firm's communications balance specific claims of investment benefits from a securities product or service (especially complex products) with the key risks specific to that product or service?
  - Do your firm's communications contain predictions or projections of investment performance to investors that are generally prohibited by FINRA Rule 2210(d)(1)(F)?

▶ **Mobile Apps –**
  - Has your firm established and implemented a comprehensive supervisory system for communications through mobile apps?
  - Have you tested the accuracy of account information, including labels and data, displayed in your mobile apps?
  - Do your mobile apps accurately describe how their features work?
  - Do your mobile apps identify information in ways that are readily understandable, based on the experience level of your customers?
  - Do your mobile apps provide investors with readily available information to explain complex strategies and investments and associated risks?
  - If your firm offers an app to retail customers, does the information provided to customers constitute a “recommendation” that would be covered by Reg BI, and in the case of recommendations of options or variable annuities, FINRA Rules 2360 (Options) or 2330 (Members’ Responsibilities Regarding Deferred Variable Annuities)? If so, how does your firm comply with these obligations?

▶ **Digital Communication Channels –**
  - Does your firm's digital communication policy address all permitted and prohibited digital communication channels and features available to your customers and associated persons?
  - Does your firm review for red flags that may indicate a registered representative is communicating through unapproved communication channels, and does your firm follow up on such red flags? For example, red flags might include email chains that copy unapproved representative email addresses, references in emails to communications that occurred outside approved firm channels or customer complaints mentioning such communications.
  - How does your firm supervise and maintain books and records in accordance with SEC and FINRA Books and Records Rules for all approved digital communications?
  - Does your firm have a process to confirm that all business-related communications comply with the content standards set forth in FINRA Rule 2210?

▶ **Digital Asset Communications –** If your firm or an affiliate engages in digital asset activities:
  - do your firm provide a fair and balanced presentation in marketing materials and retail communications, including addressing risks presented by digital asset investments and not misrepresenting the extent to which digital assets are regulated by FINRA or the federal securities laws or eligible for protections thereunder, such as Securities Investor Protection Corporation (SIPC) coverage?
• do your firm’s communications misleadingly imply that digital asset services offered through an affiliated entity are offered through and under the supervision, clearance and custody of a registered broker-dealer?

▲ Cash Management Accounts Communications – If your firm offers Cash Management Accounts, does it:
  • clearly communicate the terms of the Cash Management Accounts?
  • disclose that the Cash Management Accounts’ deposits are obligations of the destination bank and not cash balances held by your firm?
  • assure that its communications do not state or imply that:
    • brokerage accounts are similar to or the same as bank “checking and savings accounts” or other accounts insured by the Federal Deposit Insurance Corporation (FDIC); and
    • FDIC insurance coverage applies to funds when held at a registered broker-dealer?
  • review whether communications fairly explain the:
    • nature and structure of the program;
    • relationship of the brokerage accounts to any partner banks in the Cash Management Accounts;
    • amount of time it may take for customer funds to reach the bank accounts; and
    • benefits and risks of participating in such programs?

▲ Municipal Securities Communications – If your firm offers municipal securities, does it confirm that advertisements for such securities include the necessary information to be fair, balanced and not misleading, and do not include:
  • exaggerated claims about safety or misleading comparisons to US Treasury Securities;
  • statements claiming “direct access” to bonds in the primary market if the firm is not an underwriter; and
  • unwarranted claims about the predictability or consistency of growth or payments?

▲ If an advertisement includes claims of municipal securities being “tax free,” does it also explain any applicable state, local, alternative minimum tax, capital gains or other tax consequences?

▲ If an advertisement advertises a “taxable equivalent” yield on a municipal security offering, does it provide sufficient information regarding the tax bracket used to make the calculation?

Exam Findings and Effective Practices

Exam Findings:

▲ False, Misleading and Inaccurate Information in Mobile Apps –
  • Incorrect or misleading account balances or inaccurate information regarding accounts’ historical performance.
  • Sending margin call warnings to customers whose account balances were not approaching, or were below, minimum maintenance requirements.
  • Falsely informing customers that their accounts were not enabled to trade on margin, when the accounts were, in fact, margin enabled.
  • Misstating the risk of loss associated with certain options transactions.
  • Distributing false and misleading promotions through social media and “push” notifications on mobile apps that made promissory claims or omitted material information.
Deficient Communications Promoting Digital Assets –
  - Falsely identifying the broker-dealer as the entity from whom digital assets may be purchased or creating confusion about which entity is offering digital assets by using identical or substantially similar names to the broker dealer’s name.

Misrepresentations in Cash Management Account Communications –
  - Misleading statements or claims that either state or imply the broker-dealer is a bank.
  - Misleading or false claims that state or imply the Cash Management Accounts are “checking and savings accounts.”
  - Inaccurate or misleading statements concerning the amount of FDIC insurance coverage provided to investor funds when they are held at a partner bank.
  - Incomplete or inaccurate claims concerning the amount of time it may take for customer funds to reach the bank accounts or be available to investors once deposited at a partner bank.
  - Inaccurate or misleading claims about the actual terms of the Cash Management Accounts.
  - Failure to balance promotional claims with the risks of participating in such programs.

Insufficient Supervision and Recordkeeping for Digital Communications – Not maintaining policies and procedures to reasonably identify and respond to red flags—such as customer complaints, representatives’ email, OBA reviews or advertising reviews—that registered representatives used business-related digital communications methods not controlled by the firm, including texting, messaging, social media, collaboration apps or “electronic sales seminars” in chatrooms.

No WSPs and Controls for Communication That Use Non-Member or OBA Names (so-called “Doing Business As” or “DBA” Names) –
  - Not maintaining WSPs to identify the broker-dealer clearly and prominently as the entity through which securities were offered in firm communications, such as websites, social media posts, seminars or emails that promote or discuss the broker-dealer’s securities business and identify a non-member entity, such as a representative's OBA.
  - Not including a “readily apparent reference” and hyperlink to FINRA’s BrokerCheck in such communications.

Municipal Securities Advertisements – Using false and misleading statements or claims about safety, unqualified or unwarranted claims regarding the expertise of the firm, and promissory statements and claims regarding portfolio growth.

Effective Practices:

Comprehensive Procedures for Mobile Apps – Maintaining and implementing comprehensive procedures for the supervision of mobile apps, for example, that confirm:
  - data displayed to customers is accurate; and
  - information about mobile apps’ tools and features complies with FINRA’s communications and other relevant rules before it is posted to investors.

Comprehensive Procedures for Digital Communications – Maintaining and implementing procedures for supervision of digital communication channels, including:
  - Monitoring of New Tools and Features – Monitoring new communication channels, apps and features available to their associated persons and customers.
• **Defining and Enforcing What is Permissible and Prohibited** – Clearly defining permissible and prohibited digital communication channels and blocking prohibited channels, tools or features, including those that prevent firms from complying with their recordkeeping requirements.

• **Supervision** – Implementing supervisory review procedures tailored to each digital channel, tool and feature.

• **Video Content Protocols** – Developing WSPs and controls for live-streamed public appearances, scripted presentations or video blogs.

• **Training** – Implementing mandatory training programs prior to providing access to firm-approved digital channels, including expectations for business and personal digital communications and guidance for using all permitted features of each channel.

• **Disciplinary Action** – Temporarily suspending or permanently blocking from certain digital channels or features those registered representatives who did not comply with the policies and requiring them to take additional digital communications training.

▶ **Digital Asset Communications** – Maintaining and implementing procedures for firm digital asset communications, including:

  • **Risk Disclosure** – Prominently describing the risks associated with digital assets that are needed to balance any statements or claims contained in a digital asset communication, including that such investments are speculative, involve a high degree of risk, are generally illiquid, may have no value, have limited regulatory certainty, are subject to potential market manipulation risks and may expose investors to loss of principal.

  • **Communication Review** – Reviewing firms’ communications to confirm that they were not exaggerating the potential benefits of digital assets or overstating the current or future status of digital asset projects or platforms.

  • **Communication to Differentiate Digital Assets From Broker-Dealer Products** – Identifying, segregating and differentiating firms’ broker-dealer products and services from those offered by affiliates or third parties, including digital asset affiliates; and clearly and prominently identifying entities responsible for non-securities digital assets businesses (and explaining that such services were not offered by the broker-dealer or subject to the same regulatory protections as those available for securities).

▶ **Reviews of Firms’ Capabilities for Cash Management Accounts** – Requiring new product groups or departments to conduct an additional review for proposed Cash Management Accounts to confirm that the firms’ existing business processes, supervisory systems and compliance programs—especially those relating to communications—can support such programs.

▶ **Use of Non-Member or OBA Names (so-called DBAs)** – Maintaining and implementing procedures for OBA names, including:

  • **Prior Approval** – Prohibiting the use of OBA communications that concern the broker-dealer’s securities business without prior approval by compliance and creating a centralized system for the review and approval of such communications, including content and disclosures.

  • **Training** – Providing training on relevant FINRA rules and firm policies and requiring annual attestations to demonstrate compliance with such requirements.

  • **Templates** – Requiring use of firm-approved vendors to create content or standardized templates populated with approved content and disclosures for all OBA communications (including websites, social media, digital content or other communications) that also concern the broker-dealer’s securities business.

  • **Notification and Monitoring** – Requiring registered representatives to notify compliance of any changes to approved communications and conducting periodic, at least annual, monitoring and review of previously approved communications for changes and updates.
Municipal Securities Advertisements – Maintaining and implementing procedures for firm municipal securities communications, including:

- Prior Approval – Requiring prior approval of all advertisements concerning municipal securities by an appropriately qualified principal to confirm the content complies with applicable content standards.
- Training – Providing education and training for firm personnel on applicable FINRA and MSRB rules and firm policies.
- Risk Disclosure – Balancing statements concerning the benefits of municipal securities by prominently describing the risks associated with municipal securities, including credit risk, market risk and interest rate risk.
- Review – Reviewing firms’ communications to confirm that the potential benefits of tax features are accurate and not exaggerated.

Additional Resources

- Regulatory Notice 21-25 (FINRA Continues to Encourage Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- Regulatory Notice 20-21 (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- Regulatory Notice 19-31 (Disclosure Innovations in Advertising and Other Communications with the Public)
- Regulatory Notice 17-18 (Guidance on Social Networking Websites and Business Communications)
- Regulatory Notice 11-39 (Social Media Websites and the Use of Personal Devices for Business Communications)
- Regulatory Notice 10-06 (Guidance on Blogs and Social Networking Web Sites)
- Advertising Regulation Topic Page
- FINRA’s Social Media Topic Page
- MSRB Notice 2019-07
- MSRB Notice 2018-18

Private Placements

Regulatory Obligations and Related Considerations

Regulatory Obligations:

In Regulatory Notice 10-22 (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings), FINRA noted that members that recommend private offerings have obligations under FINRA Rule 2111 (Suitability) and FINRA Rule 3110 (Supervision) to conduct reasonable diligence by evaluating “the issuer and its management; the business prospects of the issuer; the assets held by or to be acquired by the issuer; the claims being made; and the intended use of proceeds of the offering.” Although FINRA’s Suitability Rule continues to apply to recommendations to non-retail customers, it no longer applies to recommendations to retail customers. Instead, the SEC’s Reg BI applies to recommendations to retail customers of any securities transaction or investment strategy involving securities, including recommendations of private offerings.
Additionally, firms must make timely filings for specified private placement offerings with FINRA’s Corporate Financing Department under FINRA Rules 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities), and should also be aware of recent amendments to these rules.  

Related Considerations:

- What policies and procedures does your firm have to address filing requirements and timelines under FINRA Rules 5122 and 5123? How does it review for compliance with such policies?
- How does your firm confirm that associated persons conduct reasonable diligence prior to recommending private placement offerings, including conducting further inquiry into red flags?
- How does your firm address red flags regarding conflicts of interest identified during the reasonable diligence process and in third-party due diligence reports?
- How does your firm manage the transmission of funds and amended terms in contingency offerings, including ensuring compliance with Securities Exchange Act Rules 10b-9 and 15c2-4, as applicable?

Exam Findings and Effective Practices

Exam Findings:

- **Late Filings** – Not having policies and procedures, processes and supervisory programs to comply with filing requirements; and failing to make timely filings (with, in some cases, delays lasting as long as six to 12 months after the offering closing date).
- **No Reasonable Diligence** – Failing to perform reasonable diligence of private placement offerings prior to recommending them to retail investors, including:
  - failing to conduct an appropriate level of research, particularly when the firm lacks experience or specialized knowledge pertaining to an issuer’s underlying business or when an issuer lacks an operating history;
  - relying unreasonably on the firm’s experience with the same issuer in previous offerings; and
  - failing to inquire into and analyze red flags identified during the reasonable-diligence process or in third-party due diligence reports.

Effective Practices:

- **Private Placement Checklist** – Creating checklists with—or adding to existing due diligence checklists—all steps, filing dates and related documentation requirements, noting staff responsible for performing functions and tasks and evidence of supervisory principal approval for the reasonable diligence process and the filing requirements of FINRA Rules 5122 and 5123.
- **Independent Research** – Conducting and documenting independent research on material aspects of the offering; identifying any red flags with the offering or the issuer (such as questionable business plans or unlikely projections or results); and addressing and, if possible, resolving concerns that would be deemed material to a potential investor (such as liquidity restrictions).
- **Independent Verification** – Verifying information that is key to the performance of the offering (such as unrealistic costs projected to execute the business plan, coupled with aggressively projected timing and overall rate of return for investors), in some cases with support from law firms, experts and other third-party vendors.
Identifying Conflicts of Interest – Using firms’ reasonable diligence processes to identify conflicts of interest (e.g., firm affiliates or issuers whose control persons were also employed by the firm) and then addressing such conflicts (such as by confirming that the issuer prominently and comprehensively discloses these conflicts in offering documents or mitigating them by removing financial incentives to recommend a private offering over other more appropriate investments).

Responsibility for Reasonable Diligence and Compliance – Assigning responsibility for private placement reasonable diligence and compliance with filing requirements to specific individual(s) or team(s) and conducting targeted, in-depth training about the firms’ policies, process and filing requirements.

Alert System – Creating a system that alerts responsible individual(s) and supervisory principal(s) about upcoming and missed filing deadlines.

Post-Closing Assessment – Conducting reviews after the offering closes to ascertain whether offering proceeds were used in a manner consistent with the offering memorandum.

Additional Resources

- **Regulatory Notice 21-26** (FINRA Amends Rules 5122 and 5123 Filing Requirements to Include Retail Communications That Promote or Recommend Private Placements)
- **Regulatory Notice 21-10** (FINRA Updates Private Placement Filer Form Pursuant to FINRA Rules 5122 and 5123)
- **Regulatory Notice 20-21** (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- **Regulatory Notice 10-22** (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings)
- Report Center – Corporate Financing Report Cards
- FAQs about Private Placements
- Corporate Financing Private Placement Filing System User Guide
- Private Placements Topic Page
Conservation Donation Transactions Risks

FINRA is seeing continued syndications of Conservation Donation Transactions (CDTs) investment programs among broker-dealers. CDTs commonly involve private placement offerings where investor returns are based on a share of tax savings from a charitable donation. In practice, CDTs involve unrelated investors acquiring an interest in a passsthrough entity (i.e., a partnership or limited liability company) owning unimproved land. Before year-end, the passsthrough entity either grants a conservation easement—which forever limits future development of the land—or outright donates the land to a land trust. In exchange, the passsthrough entity receives charitable donation tax deductions, which serve as a return on investment to investors and often have values based solely on land appraisals that are predicated on an alternative plan to develop the land, oftentimes the equivalent of four to more than 10 times the price paid to acquire the land. (Common CDTs involve syndicated conservation easement transactions (SCETs) or substantially similar, fee simple donations of land.)

Firms that engage in CDTs should consider the following questions to determine whether they meet regulatory obligations:

- Do the CDT sponsor, appraiser or other related service providers have any prior, adverse audit history?
- Do your firm's offering disclosures present potential conflicts of interest among sponsors, consultants, land developers, prior landowners, broker-dealers, and registered persons having employment or affiliated relationships?
- In compliance with Reg BI, does your firm:
  - consider reasonably available alternatives to any recommendation of CDTs (i.e., the Care Obligation);
  - have policies and procedures to identify and—at a minimum—disclose or eliminate all conflicts of interest associated with the recommendation (i.e., the Conflicts of Interest Obligation); and
  - have policies and procedures to identify and mitigate any conflicts of interest associated with recommendations of CDTs that create an incentive for an associated person to place the interest of the firm or the associated person ahead of the retail customer's interest?
- In compliance with SEA Rule 15c2-4, does your firm promptly transmit funds to either an escrow agent or a separate bank account (as CDTs are typically associated with contingent offerings)?
- How does your firm establish and document reasonable diligence of CDTs, including further inquiries in the presence of red flags (e.g., CDTs resulting in donation deductions that are more than two-and-one-half times an investor's investment, concerns surfaced in third-party due diligence reports, large markups associated with land acquisition, certain types of fees to related parties, marketing communications promoting CDTs solely on their tax benefits)?

For additional guidance, please refer to these resources:

- Internal Revenue Service, [IRS increases enforcement action on Syndicated Conservation Easements](https://www.irs.gov) (Nov. 12, 2019)
- Land Trust Alliance, [Important Advisory: Tax Shelter Abuse of Conservation Donations](https://www.landtrustalliance.org) (Feb. 1, 2018)
Variable Annuities

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 2330 (Members’ Responsibilities Regarding Deferred Variable Annuities) establishes sales practice standards regarding recommended purchases and exchanges of deferred variable annuities. To the extent that a broker-dealer or associated person is recommending a purchase or exchange of a deferred variable annuity to a retail customer, Reg BI's obligations, discussed above, also would apply.

In addition, Rule 2330 requires firms to establish and maintain specific written supervisory procedures reasonably designed to achieve compliance with the rule. Firms must implement surveillance procedures to determine if any associated person is effecting deferred variable annuity exchanges at a rate that might suggest conduct inconsistent with FINRA Rule 2330 and any other applicable FINRA rules or the federal securities laws.

Related Considerations:

- How does your firm review for rates of variable annuity exchanges (i.e., does your firm use any automated tools, exception reports or surveillance reports)?
- Does your firm have standardized review thresholds for rates of variable annuity exchanges?
- Does your firm have a process to confirm its variable annuity data integrity (including general product information, share class, riders and exchange-based activity) and engage with affiliate and non-affiliate insurance carriers to address inconsistencies in available data, data formats and reporting processes for variable annuities?
- How do your firm's WSPs support a determination that a variable annuity exchange has a reasonable basis? How do you obtain, evaluate and record relevant information, such as:
  - loss of existing benefits;
  - increased fees or charges;
  - surrender charges, or the establishment or creation of a new surrender period;
  - consistency of customer liquid net worth invested in the variable annuity with their liquidity needs;
  - whether a share class is in the customer's best interest, given his or her financial needs, time horizon and riders included with the contract; and
  - prior exchanges within the preceding 36 months?
- Do your firm's policies and procedures require registered representatives to inform customers of the various features of recommended variable annuities such as surrender charges, potential tax penalties, various fees and costs, and market risk?
- What is the role of your registered principals in supervising variable annuity transactions, including verifying how the customer would benefit from certain features of deferred variable annuities (e.g., tax-deferral, annuitization, or a death or living benefit)? What processes, forms, documents and information do the firm's registered principals rely on to make such determinations?
- **What is your firm’s process to supervise registered representatives who advise their clients’ decisions whether or not to accept a buyout offer?**
Exam Findings and Effective Practices

Exam Findings:

- **Exchanges** – Not reasonably supervising recommendations of exchanges for compliance with FINRA Rule 2330 and Reg BI, leading to exchanges that were inconsistent with the customer’s objectives and time horizon and resulted in, among other consequences, increased fees to the customer or the loss of material, paid-for accrued benefits.

- **Insufficient Training** – Not conducting training for registered representatives and supervisors regarding how to assess costs and fees, surrender charges and long-term income riders to determine whether exchanges were suitable for customers.

- **Poor and Insufficient Data Quality** – Not collecting and retaining key information on variable annuity transactions, particularly in connection with exchange transactions; relying on processes for data collection and retention in situations where the volume of variable annuity transactions renders these processes ineffective; and failing to address inconsistencies in available data for variable annuities, as well as data formats and reporting processes.

- **Issuer Buyouts** – Not reasonably supervising recommendations related to issuer buyout offers (e.g., associated persons’ recommendations that investors surrender the contract in order to generate an exchange or new purchase) for compliance with FINRA Rule 2230 and Reg BI.

Effective Practices:

- **Automated Surveillance** – Using automated tools, exception reports and surveillance to review variable annuity exchanges; and implementing second-level supervision of supervisory reviews of exchange-related exception reports and account applications.

- **Rationales** – Requiring registered representatives to provide detailed written rationales for variable annuity exchanges for each customer (including confirming that such rationales address the specific circumstances for each customer and do not replicate rationales provided for other customers); and requiring supervisory principals to verify the information provided by registered representatives, including product fees, costs, rider benefits and existing product values.

- **Review Thresholds** – Standardizing review thresholds for rates of variable annuity exchanges; and monitoring for emerging trends across registered representatives, customers, products and branches.

- **Automated Data Supervision** – Creating automated solutions to synthesize variable annuity data (including general product information, share class, riders and exchange-based activity) in situations warranted by the volume of variable annuity transactions.

- **Data Integrity** – Engaging with insurance carriers (affiliated and non-affiliated) and third-party data providers (e.g., DTCC and consolidated account report providers) to address inconsistencies in available data, data formats and reporting processes for variable annuities.

- **Data Acquisition** – Establishing a supervisory system that collects and utilizes key transaction data, including, but not limited to:
  - transaction date;
  - rep name;
  - customer name;
  - customer age;
  - investment amount;
  - whether the transaction is a new contract or an additional investment;
  - contract type (qualified vs. non-qualified);
- contract number;
- product issuer;
- product name;
- source of funds;
- exchange identifier;
- share class; and
- commissions.

Data Analysis – Considering the following data points when conducting a review of an exchange transaction under FINRA Rule 2330 and Reg BI:
- branch location;
- customer state of residence;
- policy riders;
- policy fees;
- issuer of exchanged policy;
- exchanged policy product name;
- date exchanged policy was purchased;
- living benefit value, death benefit value or both, that was forfeited;
- surrender charges incurred; and
- any additional benefits surrendered with forfeiture.

Additional Resources

SEC
- Regulation Best Interest, Form CRS and Related Interpretations

FINRA
- Regulation Best Interest (Reg BI) Topic Page
- Regulatory Notice 20-18 (FINRA Amends Its Suitability, Non-Cash Compensation and Capital Acquisition Broker (CAB) Rules in Response to Regulation Best Interest)
- Regulatory Notice 20-17 (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- Regulatory Notice 10-05 (FINRA Reminds Firms of Their Responsibilities Under FINRA Rule 2330 for Recommended Purchases or Exchanges of Deferred Variable Annuities)
- Notice to Members 07-06 (Special Considerations When Supervising Recommendations of Newly Associated Registered Representatives to Replace Mutual Funds and Variable Products)
- Notice to Members 99-35 (The NASD Reminds Members of Their Responsibilities Regarding the Sales of Variable Annuities)
- Variable Annuities Topic Page
Market Integrity

Consolidated Audit Trail (CAT)

Regulatory Obligations and Related Considerations

Regulatory Obligations:
FINRA and the national securities exchanges have adopted rules requiring their members to comply with Exchange Act Rule 613 and the CAT NMS Plan FINRA Rule 6800 Series (Consolidated Audit Trail Compliance Rule) (collectively, CAT Rules), which cover reporting to the CAT; clock synchronization; time stamps; connectivity and data transmission; development and testing; recordkeeping; and timeliness, accuracy and completeness of data requirements. Regulatory Notice 20-31 (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT) describes practices and recommended steps firms should consider when developing and implementing their CAT Rules compliance program.

Related Considerations:
- Do your firm’s CAT Rules WSPs: (1) identify the individual, by name or title, responsible for the review of CAT reporting; (2) describe specifically what type of review(s) will be conducted of the data posted on the CAT Reporter Portal; (3) specify how often the review(s) will be conducted; and (4) describe how the review(s) will be evidenced?
- How does your firm confirm that the data your firm reports, or that is reported on your firm’s behalf, is transmitted in a timely fashion and is complete and accurate?
- How does your firm determine how and when clocks are synchronized, who is responsible for clock synchronization, how your firm evidences that clocks have been synchronized and how your firm will self-report clock synchronization violations?
- Does your firm conduct daily reviews of the Industry Member CAT Reporter Portal (CAT Reporter Portal) to review file status to confirm the file(s) sent by the member or by their reporting agent was accepted by CAT and to identify and address any file submission or integrity errors?
- Does your firm conduct periodic comparative reviews of accepted CAT data against order and trade records and the CAT Reporting Technical Specifications?
- Does your firm communicate regularly with your CAT reporting agent, review relevant CAT guidance and announcements and report CAT reporting issues to the FINRA CAT Help Desk?
- Does your firm maintain the required CAT order information as part of its books and records and in compliance with FINRA Rule 6890 (Recordkeeping)?
- How does your firm work with its clearing firm and third-party vendors to maintain CAT compliance?

Exam Findings and Effective Practices

Exam Findings:
- Inaccurate Reporting of CAT Orders – Submitting information that was incorrect, incomplete or both to the Central Repository, such as:
  - account holder type;
  - buy/sell side;
  - cancel quantity;
  - route event quantity (e.g., reporting an old quantity that had been modified to a different amount);
- trading session code;
- new order code;
- department type code (e.g., reporting “A” for agent, when the firm does not execute orders);
- time in force;
- handling instructions (e.g., reporting new order events as Stop on Quote (SOQ) or Stop Limit on Quote (SLQ)); and
- representative indicator (i.e., reporting the representative indicator to reflect a representative order when the order in a firm account was not created for the purpose of working one or more customer or client orders).

- Late Resolution of Repairable CAT Errors – Not resolving repairable CAT errors in a timely manner (i.e., within the T+3 requirement).
- Inadequate Vendor Supervision – Not establishing and maintaining WSPs or supervisory controls regarding both CAT reporting and clock synchronization that are performed by third-party vendors.

Effective Practices:
- Supervision – Implementing a comparative review of CAT submissions versus firm order records; and utilizing CAT Report Cards and CAT FAQs to design an effective supervision process.
- Clock Synchronization Related to Third Parties – Obtaining adequate information from third parties to meet applicable clock synchronization requirements.13

Additional Resources
- CAT NMS Plan
- FINRA
  - Consolidated Audit Trail (CAT) Topic Page
  - Equity Report Cards
  - Regulatory Notice 20-31 (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT)
  - Regulatory Notice 19-19 (FINRA Reminds Firms to Register for CAT Reporting by June 27, 2019)
  - Regulatory Notice 17-09 (The National Securities Exchanges and FINRA Issue Joint Guidance on Clock Synchronization and Certification Requirements Under the CAT NMS Plan)

Best Execution

Regulatory Obligations and Related Considerations

Regulatory Obligations:
FINRA Rule 5310 (Best Execution and Interpositioning) requires that, in any transaction for or with a customer or a customer of another broker-dealer, a member firm and persons associated with a member firm shall use reasonable diligence to ascertain the best market for the subject security and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions. Where a firm may choose to not conduct an order-by-order review—to the extent consistent with Rule 5310 and associated guidance—it must have procedures in place to confirm it periodically conducts “regular and rigorous” reviews of the execution quality of its customers’ orders.
Best execution obligations apply to any member firm that receives customer orders—for purposes of handling and execution—including firms that receive orders directly from customers, as well as those that receive customer orders from other firms for handling and execution, such as wholesale market makers. These obligations also apply when a firm acts as agent for the account of its customer and executes transactions as principal. Any firm subject to FINRA Rule 5310 cannot transfer its duty of best execution to another person; additionally, any firm that routes all of its customer orders to another firm without conducting an independent review of execution quality would violate its duty of best execution.

Related Considerations:
- How does your firm determine whether to employ order-by-order or “regular and rigorous” reviews of execution quality?
- If applicable, how does your firm implement and conduct an adequate “regular and rigorous” review of the quality of the executions of its customers’ orders and orders from a customer of another broker-dealer?
- If applicable, how does your firm document its “regular and rigorous” reviews, the data and other information considered, order routing decisions and the rationale used, and address any deficiencies?
- How does your firm compare the execution quality received under its existing order routing and execution arrangements (including the internalization of order flow) to the quality of the executions it could obtain from competing markets (whether or not the firm already has routing arrangements with them), including off-exchange trading venues?
- How does your firm address potential conflicts of interest in order routing decisions, including those involving:
  - affiliated entities (e.g., affiliated broker-dealers, affiliated alternative trading systems (ATSs));
  - market centers, including off-exchange trading venues, that provide payment for order flow (PFOF) or other order-routing inducements; and
  - orders from customers of another broker-dealer for which your firm provides PFOF?
- If your firm provides PFOF to another broker-dealer, how does your firm prevent those payments from interfering with your firm’s best execution obligations (including situations where you provide PFOF and execute the covered orders)?
- If your firm engages in fixed income and options trading, has it established targeted policies and procedures to address its best execution obligations for these products?
- Does your firm consider differences among security types within these products, such as the different characteristics and liquidity of U.S. Treasury securities compared to other fixed income securities?
- How does your firm meet its best execution obligations with respect to trading conducted in both regular and extended trading hours?
- Does your firm consider the risk of information leakage affecting pricing when assessing the execution quality of orders routed to a particular venue?
- What data sources does your firm use for its routing decisions and execution quality reviews for different order types and sizes, including odd lots?
- How does your firm handle fractional share investing in the context of its best execution obligations?

Exam Findings and Effective Practices

Exam Findings:
- No Assessment of Execution in Competing Markets – Not comparing the quality of the execution obtained via firms’ existing order-routing and execution arrangements against the quality of execution they could have obtained from competing markets.
No Review of Certain Order Types - Not conducting adequate reviews on a type-of-order basis, including, for example, on market, marketable limit, or non-marketable limit orders.

No Evaluation of Required Factors – Not considering certain factors set forth in Rule 5310 when conducting a “regular and rigorous review,” including, among other things, speed of execution, price improvement and the likelihood of execution of limit orders; and using routing logic that was not necessarily based on quality of execution.

Conflicts of Interest – Not considering and addressing potential conflicts of interest relating to routing orders to affiliated broker-dealers, affiliated ATSs, or market centers that provide routing inducements, such as PFOF from wholesale market makers and exchange liquidity rebates.

Targeted Reviews of Wholesale Market Makers
FINRA is conducting targeted best execution reviews of wholesale market makers concerning their relationships with broker-dealers that route orders to them as well as their own order routing practices and decisions (with respect to these orders). These targeted reviews are evaluating:

- whether wholesale market makers are conducting adequate execution quality reviews;
- whether order routing, handling and execution arrangements (including PFOF agreements) with retail broker-dealers have an impact on the wholesale marker makers’ order handling practices and decisions, and fulfillment of their best execution obligations; and
- any modified order handling procedures that the wholesale market makers implemented during volatile or extreme market conditions.

Effective Practices:

- Exception Reports – Using exception reports and surveillance reports to support firms’ efforts to meet their best execution obligations.

- PFOF Order Handling Impact Review – Reviewing how PFOF affects the order-handling process, including the following factors: any explicit or implicit contractual arrangement to send order flow to a third-party broker-dealer; terms of these agreements; whether it is on a per-share basis or per-order basis; and whether it is based upon the type of order, size of order, type of customer or the market class of the security.

- Risk-Based “Regular and Rigorous Reviews” – Conducting “regular and rigorous” reviews, at a minimum, on a quarterly or more frequent basis (such as monthly), depending on the firm’s business model.

- Continuous Updates – Updating WSPs and best execution analysis to address market and technology changes.

Additional Resources

- Regulatory Notice 21-23 (FINRA Reminds Member Firms of Requirements Concerning Best Execution and Payment for Order Flow)

- Regulatory Notice 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions)

- Regulatory Notice 15-46 (Guidance on Best Execution Obligations in Equity, Options and Fixed Income Markets)

- Notice to Members 01-22 (NASD Regulation Reiterates Member Firm Best Execution Obligations And Provides Guidance to Members Concerning Compliance)

- FINRA Report Center

- Equity Report Cards

- Best Execution Outside-of-the-Inside Report Card
Disclosure of Routing Information  
NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:
Rule 606 of Regulation NMS requires broker-dealers to disclose information regarding the handling of their customers’ orders in NMS stocks and listed options. These disclosures are designed to help customers: better understand how their firm routes and handles their orders; assess the quality of order handling services provided by their firm; and ascertain whether the firm is effectively managing potential conflicts of interest that may impact their firm’s routing decisions.

Related Considerations:
- Does the firm publish accurate, properly formatted quarterly routing reports on its website for the required retention period as specified under Rule 606(a), including use of the SEC’s most recently published PDF and XML schema?
- If the firm is not required to publish a quarterly report under Rule 606(a), does the firm have an effective supervisory process to periodically confirm that the firm has no orders subject to quarterly reporting?
- If the firm routes orders to non-exchange venues, does the firm adequately assess whether such venues are covered under Rule 606(a)?
- If the firm routes orders to non-exchange venues, does the firm obtain and retain sufficient information from such venues to properly report the material terms of its relationships with such venues, including specific quantitative and qualitative information regarding PFOF and any profit-sharing relationship?
- If the firm claims an exemption from providing not held order reports under Rule 606(b)(3) pursuant to Rule 606(b)(4) or (5), what policies and procedures does the firm have in place to determine if the firm’s or a customer’s order activity falls below the relevant de minimis thresholds?
- If the firm is required to provide customer-specific disclosures under Rule 606(b)(3), does the firm provide accurate, properly formatted disclosures for the prior six months to requesting customers within seven business days of receiving the request?

Exam Findings and Effective Practices

Exam Findings:
- Inaccurate Quarterly Reports – Publishing inaccurate information in the quarterly report on order routing, such as:
  - reporting only held orders in listed options, instead of both held and not held orders;
  - incorrectly stating that the firm does not have a profit-sharing arrangement or receive PFOF from execution venues;
  - not including payments, credits or rebates (whether received directly from an exchange or through a pass-through arrangement) in the “Net Payment Paid/Received” and “Material Aspects” sections of the quarterly report;
  - not including exchange pricing arrangements (e.g., tiered pricing) in the “Net Payment Paid/Received” and “Material Aspects” sections of the quarterly report;
  - not disclosing any amounts of “Net Payment Paid/Received”, when the firm receives PFOF for at least one of the four order types (i.e., Market Orders, Marketable Limit Orders, Non-Marketable Limit Orders, Other Orders);
  - inaccurately identifying reported execution venues as “Unknown”;
  - inaccurately identifying firms as execution venues (e.g., identifying routing broker-dealer as execution venue, rather than the exchange where transactions are actually executed);
incorrectly listing an entity as an execution venue when that entity does not execute trades (e.g., firm that re-routes, but does not execute, orders; options consolidator that does not provide liquidity); and
not posting the quarterly report on their firm’s website in both required formats (i.e., PDF and XML schema).

**Incomplete Disclosures** – Not adequately describing material aspects of their relationships with disclosed venues in the Material Aspects disclosures portion of the quarterly report, such as:

- inadequate descriptions of specific terms of PFOF and other arrangements (e.g., “average” amounts of PFOF rather than specific disclosure noting the payment types, specific amount received for each type of payment, terms and conditions of each type of payment);
- ambiguous descriptions of receipt of PFOF (e.g., firm “may” receive payment);
- inadequate or incomplete descriptions of PFOF received through pass-through arrangements;
- incomplete descriptions of exchange credits or rebates; and
- incomplete descriptions of tiered pricing arrangements, including the specific pricing received by the firm.

**Deficient Communications** – Not notifying customers in writing of the availability of information specified under Rule 606(b)(1), as required by Rule 606(b)(2).15

**Insufficient WSPs** – Either not establishing or not maintaining adequate WSPs reasonably designed to achieve compliance with the new requirements of Rule 606, including:

- not updating their Disclosure of Order Routing Information WSPs to include new requirements detailed in amended Rule 606(a)(1) or new Rule 606(b)(3);
- not describing the steps taken to review whether firms verified the data integrity of information sent to, or received from, their vendor—or not stating how the review would be evidenced by the reviewer;
- not articulating a supervisory method of review to verify the accuracy, format, completeness, timely processing and details of the new Rule 606(b)(3) report, if requested, as well as documenting the performance of that review; and
- not requiring the inclusion of detailed information regarding the routing and execution of the firm’s customers’ listed options orders in quarterly reports or customer-requested order routing disclosures.

**Effective Practices:**

**Supervision** – Conducting regular, periodic supervisory reviews of the public quarterly reports and customer-specific order disclosure reports, if applicable, for accuracy (e.g., assuring that per-venue disclosures of net aggregate PFOF and other payments are accurately calculated) and completeness (e.g., assuring that the Material Aspects section adequately describes the firm’s PFOF and other payment arrangement for each execution venue, including all material aspects that may influence the firm’s order routing decisions).

**Due Diligence on Vendors** – Performing due diligence to assess the accuracy of public quarterly reports and customer-specific order disclosure reports provided by third-party vendors by, for example, holding periodic meetings with vendors to review content of reports, comparing order samples against vendor-provided information, and confirming with the vendor that all appropriate order information is being received (particularly when the firm has complex routing arrangements with execution venues).

**Additional Resources**

- SEC’s [Responses to Frequently Asked Questions Concerning Rule 606 of Regulation NMS](https://www.sec.gov/divisions/occ/factssheets/606factsheet.pdf)
- SEC’s [Staff Legal Bulletin No. 13A: Frequently Asked Questions About Rule 11Ac1-6](https://www.sec.gov/divisions/corpfin/11ac1-6-faq.pdf)
- SEC’s [Order Routing and Handling Data Technical Specification](https://www.sec.gov/divisions/corpfin/11ac1-6-order-routing-handling-data.pdf)
Market Access Rule

Regulatory Obligations and Related Considerations

Regulatory Obligations:
Exchange Act Rule 15c3-5 (Market Access Rule) requires firms with market access or that provide market access to their customers to “appropriately control the risks associated with market access so as not to jeopardize their own financial condition, that of other market participants, the integrity of trading on the securities markets and the stability of the financial system.” The Market Access Rule applies generally to securities traded on an exchange or alternative trading system, including equities, equity options, exchange-traded funds (ETFs), debt securities, security-based swaps, security futures products, as well as digital assets that meet the SEC’s definition of a security.

Related Considerations:
- If your firm has or provides market access, does it have reasonably designed risk-management controls and WSPs to manage the financial, regulatory or other risks associated with this business activity?
- If your firm is highly automated, how does it manage and deploy technology changes for systems associated with market access and what controls does it use, such as kill switches, to monitor and respond to aberrant behavior by trading algorithms or other impactful market-wide events?
- How does your firm adjust credit limit thresholds for customers, including institutional customers (whether temporary or permanent)?
- Does your firm use any automated controls to timely revert ad hoc credit limit adjustments?
- If your firm uses third-party vendor tools to comply with its Market Access Rule obligations, does it review whether the vendor can meet the obligations of the rule?
- How does your firm maintain direct and exclusive control of applicable thresholds?
- What type of training does your firm provide to individual traders regarding the steps and requirements for requesting ad hoc credit limit adjustments?
- Does your firm test its market access controls, including fixed income controls, and how do you use that test for your firm's annual CEO certification attesting to your firm's controls?
- If your firm operates an ATS that has subscribers that are not broker-dealers, how does your firm comply with the requirements of the Market Access Rule, including establishing, documenting and maintaining a system of controls and supervisory procedures reasonably designed to manage the financial, regulatory and other risks of this business activity?

Exam Findings and Effective Practices

Exam Findings:
- **Insufficient Controls** – No pre-trade order limits, pre-set capital thresholds and duplicative and erroneous order controls for accessing ATSS, including those that transact fixed income transactions; not demonstrating the reasonability of assigned capital and credit pre-trade financial control thresholds; inadequate policies and procedures to govern intra-day changes to firms' credit and capital thresholds, including requiring or obtaining approval prior to adjusting credit or capital thresholds, documenting justifications for any adjustments and ensuring thresholds for temporary adjustments revert back to their pre-adjusted values.
- **Inadequate Financial Risk Management Controls** – For firms with market access, or those that provide it, unreasonable capital thresholds for trading desks, and unreasonable aggregate daily limits or credit limits for institutional customers and counterparties.
- **Reliance on Vendors** – Relying on third-party vendors’ tools, including those of an ATS or exchange, to apply their financial controls without performing adequate due diligence, not understanding how vendors’ controls
operate, or both; and not maintaining direct and exclusive control over controls by allowing the ATS to
unilaterally set financial thresholds for firms’ fixed income orders without the involvement of the firm,
instead of establishing their own thresholds (some firms were not sure what their thresholds were and had
no means to monitor their usage during the trading day).

Effective Practices:

- **Pre-Trade Fixed Income Financial Controls** – Implementing systemic pre-trade “hard” blocks to prevent fixed
  income orders from reaching an ATS that would cause the breach of a threshold.
- **Intra-Day Ad Hoc Adjustments** – Implementing processes for requesting, approving, reviewing and
documenting ad hoc credit threshold increases and returning limits to their original values as needed.
- **Tailored Erroneous or Duplicative Order Controls** – Tailoring erroneous or duplicative order controls to
  particular products, situations or order types, and preventing the routing of market orders based on impact
  (Average Daily Volume Control) that are set at reasonable levels (particularly in thinly traded securities); and
  calibrating to reflect, among other things, the characteristics of the relevant securities, the business of the
  firm and market conditions.
- **Post-Trade Controls and Surveillance** – When providing direct market access via multiple systems, including
  sponsored access arrangements, employing reasonable controls to confirm that those systems’ records
  were aggregated and integrated in a timely manner and conducting holistic post-trade and supervisory
  reviews for, among other things, potentially manipulative trading patterns.
- **Testing of Financial Controls** – Periodically testing their market access controls, which forms the basis for an
  annual CEO certification attesting to firms’ controls.

Additional Resources

- [Regulatory Notice 16-21](#) (SEC Approves Rule to Require Registration of Associated Persons Involved in the
  Design, Development or Significant Modification of Algorithmic Trading Strategies)
- [Regulatory Notice 15-09](#) (Guidance on Effective Supervision and Control Practices for Firms Engaging in
  Algorithmic Trading Strategies)
- FINRA’s [Algorithmic Trading Topic Page](#)
- FINRA’s [Market Access Topic Page](#)
- SEC’s [Responses to Frequently Asked Questions Concerning Risk Management Controls for Brokers or
  Dealers with Market Access](#)
Financial Management

Net Capital

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Exchange Act Rule 15c3-1 (Net Capital Rule) requires that firms must at all times have and maintain net capital at no less than the levels specified pursuant to the rule to protect customers and creditors from monetary losses that can occur when firms fail. Exchange Act Rule 17a-11 requires firms to notify FINRA in the event their net capital falls below the minimum amount required by the Net Capital Rule.

If firms have an affiliate paying any of their expenses, *Notice to Members 03-63* (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers) provides guidance for establishing an Expense Sharing Agreement that meets the standards set forth in Exchange Act Rule 17a-316; firms with office leases should apply the guidance in *Regulatory Notice 19-08* (Guidance on FOCUS Reporting for Operating Leases) for reporting lease assets and lease liabilities on their FOCUS reports. Additionally, firms must align its revenue recognition practices with the requirements of the Financial Accounting Standards Board’s Topic 606 (Revenue from Contracts with Customers).

Related Considerations:

- How does your firm review its net capital treatment of assets to confirm that they are correctly classified for net capital purposes?
- How does your firm confirm that it has correctly identified and aged all failed to deliver contracts, properly calculated the applicable net capital charges and correctly applied the deductions to its net capital calculation?
- For firms with expense-sharing agreements, what kind of allocation methodology does your firm use and what kind of documentation does your firm maintain to substantiate its methodology for allocating specific broker-dealer costs to the firm or an affiliate?

Exam Findings and Effective Practices

Exam Findings:

- **Inaccurate Classification of Receivables, Liabilities and Revenue** – Incorrectly classifying receivables, liabilities and revenues, which resulted in inaccurate reporting of firms’ financial positions and in some instances, a capital deficiency; incorrectly classifying non-allowable assets, such as large investments in certificates of deposit (CDs) because firms did not have a process to assess the net capital treatment of CDs pursuant to Exchange Act Rule 15c3-1(c)(2)(vi)(E); and not reviewing account agreements for CDs to determine whether they contained stipulations restricting withdrawals prior to maturity, including stipulations giving the bank discretion to permit or prohibit their withdrawal.

- **Failed to Deliver and Failed to Receive Contracts (Fails)** – Not having a process to correctly identify, track and age intra-month and end-of-the-month Fails for firms operating an Exchange Act Rule 15a-6 chaperoning business, including:
  - **Inaccurate Net Capital Charge** – Failing to compute and apply the correct applicable net capital charge for aged Fails;
  - **No Information from Clearing Firm** – Failing to request or confirm receipt of timely information relating to Fails from their clearing firms;
  - **Gaps in Policies and Procedures** – Failing to address monitoring, reporting and aging of Fails in firms’ policies and procedures;
  - **Incorrect Balance Sheets and FOCUS Reports** – Failing to record Fails on firms’ balance sheets, and as a result, filing incorrect FOCUS reports; and
  - **No Blotters** – Failing to maintain blotters for Fails.
FINANCIAL MANAGEMENT | NET CAPITAL

- **Incorrect Capital Charges for Underwriting Commitments** – Not maintaining an adequate process to assess moment-to-moment and open contractual commitment capital charges on underwriting commitments, and not understanding their role as it pertained to the underwriting (i.e., best efforts or firm commitment).

- **Inaccurate Recording of Revenue and Expenses** – Using cash accounting to record revenue and expenses as of the date the money changes hands, rather than accrual accounting (where firms would record revenue and expenses as of the date that revenue is earned or expenses are incurred); and making ledger entries as infrequently as once per month, as a result of which firms did not have adequate context to determine the proper accrual-based transaction date.

- **Insufficient Documentation Regarding Expense-Sharing Agreements** – Not delineating a method of allocation for payment; not allocating (fixed or variable) expenses proportionate to the benefit to the broker-dealer; or not maintaining sufficient documentation to substantiate firms’ methodologies for allocating specific broker-dealer costs—such as technology fees, marketing charges, retirement account administrative fees and employees’ compensation—to broker-dealers or affiliates.

**Effective Practices:**

- **Net Capital Assessment** – Performing an assessment of net capital treatment of assets, including CDs, to confirm that they were correctly classified for net capital purposes.

- **Agreement Review** – Obtaining from and verifying with banks the withdrawal terms of any assets, with particular focus on CD products, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset’s classification and its net capital charge for the terms of all assets, including CDs, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset’s classification and its net capital charge.

- **Training and Guidance** – Developing guidance and training for Financial and Operational Principal and other relevant staff on Net Capital Rule requirements for Fails, including how to report Fails on their balance sheets, track the age of Fails and if necessary, calculate any net capital deficit resulting from aged Fails.

- **Aging Review** – Performing reviews to confirm that they correctly aged Fail contract charges and correctly applied a net capital deduction, when applicable, to their net capital calculation.

- **Collaboration With Clearing Firms** – Clarifying WSPs to address clearing firms’ responsibilities regarding net capital requirements, including for Fails, and introducing firms engaging their clearing firms to confirm that:
  - introducing firms were receiving a record of all Fails on a daily basis (or at least monthly);
  - clearing firms’ reports included all of the required information; and
  - introducing firms were correctly interpreting the clearing firms’ reports (especially distinctions between trade date and settlement date and those dates’ implications for aging calculations for Fails).

**Additional Resources**

- **FASB**
  - [Revenue from Contracts with Customers (Topic 606)]

- **FINRA**
  - [Funding and Liquidity Topic Page]
  - [Interpretations to the SEC’s Financial and Operational Rules]
  - [Regulatory Notice 19-08 (Guidance on FOCUS Reporting for Operating Leases)]
  - [Regulatory Notice 15-33 (Guidance on Liquidity Risk Management Practices)]
  - [Regulatory Notice 10-57 (Funding and Liquidity Risk Management Practices)]
  - [Notice to Members 03-63 (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers)]
Liquidity Risk Management

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Effective liquidity controls are critical elements in a broker-dealer’s risk management framework. Exchange Act Rule 17a-3(a)(23) requires firms that meet specified thresholds to make and keep current records documenting the credit, market and liquidity risk management controls established and maintained by the firm to assist it in analyzing and managing the risks associated with its business.

FINRA routinely reviews and has shared observations on firms’ liquidity risk management practices, as discussed in Regulatory Notice 15-33 (Guidance on Liquidity Risk Management Practices) and Regulatory Notice 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions). Additionally, FINRA has adopted a new filing requirement—the Supplemental Liquidity Schedule—for firms with large customer and counterparty exposures. As noted in Regulatory Notice 21-31 (FINRA Establishes New Supplemental Liquidity Schedule (SLS)), the new SLS is designed to improve FINRA’s ability to monitor for potential adverse changes in these firms’ liquidity risk.

Related Considerations:

- What departments at your firm are responsible for liquidity management?
- How often does your firm review and adjust its assumptions regarding clearing deposits in its liquidity management plan and stress test framework?
- Does your firm’s liquidity management practices include processes for:
  - accessing liquidity during common stress conditions—such as increases in firm and client activities—as well as “black swan” events;
  - determining how the funding would be used; and
  - using empirical data from recent stress events to increase the robustness of its stress testing?
- Does your firm’s contingency funding plan take into consideration the amount of time needed to address margin calls from both customers and counterparties? Does your firm also take into consideration the type of transactions that are impacting the firm’s liquidity?
- What kind of stress tests (e.g., market or idiosyncratic) does your firm conduct? Do these tests include concentration limits within securities or sectors, and incorporate holdings across accounts held at other financial institutions?

Exam Observations and Effective Practices

Exam Observations:

- Not Modifying Business Models – Failing to incorporate the results of firms’ stress tests into their business model.
- Establishing Inaccurate Clearing Deposit Requirements – Incorrectly basing clearing deposit requirements on information that doesn’t accurately represent their business operations (e.g., using the amounts listed on FOCUS reports rather than spikes in deposit requirements that may have occurred on an intra-month basis).
- No Liquidity Contingency Plans – Failing to develop contingency plans for operating in a stressed environment with specific steps to address certain stress conditions, including identifying the firm staff responsible for enacting the plan and the process for accessing liquidity during a stress event, as well as setting standards to determine how liquidity funding would be used.
Effective Practices:

- **Liquidity Risk Management Updates** – Updating liquidity risk management practices to take into account a firm’s current business activities, including:
  - establishing governance around liquidity management, determining who is responsible for monitoring the firm’s liquidity position, how often they monitor that position and how frequently they meet as a group; and
  - creating a liquidity management plan that considers:
    - quality of funding sources;
    - potential mismatches in duration between liquidity sources and uses;
    - potential losses of counterparties;
    - how the firm obtains funding in a business-as-usual condition and stressed conditions;
    - assumptions based on idiosyncratic and market-wide conditions;
    - early warning indicators and escalation procedures if risk limits are neared or breached; and
    - material changes in market value of firm inventory over a short period of time.

- **Stress Tests** – Conducting stress tests in a manner and frequency that consider the complexity and risk of the firm’s business model, including:
  - assumptions specific to the firm’s business (e.g., increased haircuts on collateral pledged by firm, availability of funding from a parent firm) and based on historical data;
  - the firm’s sources and uses of liquidity, and if these sources can realistically fund its uses in a stressed environment;
  - the potential impact of off-balance sheet items (e.g., non-regular way settlement trades, forward contracts) on liquidity; and
  - periodic governance group review of stress tests.

Additional Resources

- **Regulatory Notice 21-31** (FINRA Establishes New Supplemental Liquidity Schedule (SLS))
- **Regulatory Notice 21-12** (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions)
- **Regulatory Notice 10-57** (Funding and Liquidity Risk Management Practices)
- FINRA’s [Funding and Liquidity Topic Page](#)

Credit Risk Management

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA has consistently reminded firms of the importance of properly managing credit risk and published *Notices* that offer guidance on effective funding and liquidity risk management practices (which are available in the “Additional Resources” section below). Risk exposures can arise from clearing arrangements, prime brokerage arrangements (especially fixed income prime brokerage), “give up” arrangements and sponsored access arrangements (discussed in the Market Access Rule section).
Further, firms should maintain a control framework where they manage credit risk and identify and address all relevant risks covering the extension of credit to their customers and counterparties. Weaknesses within the firm’s risk management and control processes could result in a firm incorrectly capturing its exposure to credit risk. In particular, Exchange Act Rule 17a-3(a)(23) requires firms that meet specified thresholds to make and keep current records documenting the credit, market and liquidity risk management controls established and maintained by the firm to assist it in analyzing and managing the risks associated with its business.

Related Considerations:

- Does your firm maintain a robust internal control framework to capture, measure, aggregate, manage, supervise and report credit risk?
- Does your firm review whether it is accurately capturing its credit risk exposure, maintain approval and documented processes for increases or other changes to assigned credit limits, and monitor exposure to affiliated counterparties?
- Does your firm have a process to confirm it is managing the quality of collateral and monitoring for exposures that would have an impact on capital?

Exam Observations and Effective Practices

Exam Observations:

- No Credit Risk Management Reviews – Not evaluating firms’ risk management and control processes to confirm whether they were accurately capturing their exposure to credit risk.
- No Credit Limit Assignments – Not maintaining approval and documentation processes for assignment, increases or other changes to credit limits.
- No Monitoring Exposure – Not monitoring exposure to firms’ affiliated counterparties.

Effective Practices:

- Credit Risk Framework – Developing comprehensive internal control frameworks to capture, measure, aggregate, manage and report credit risk, including:
  - establishing house margin requirements;
  - identifying and assessing credit exposures in real-time environments;
  - issuing margin calls and margin extensions (and resolving unmet margin calls);
  - establishing the frequency and manner of stress testing for collateral held for margin loans and secured financing transactions; and
  - having a governance process for approving new, material margin loans.
- Credit Risk Limit Changes – Maintaining approval and documentation processes for increases or other changes to assigned credit limits, including:
  - having processes for monitoring limits established at inception and on an ongoing basis for customers and counterparties;
  - reviewing how customers and counterparties adhere to these credit limits and what happens if these credit limits are breached; and
  - maintaining a governance structure around credit limit approvals.
Counterparty Exposure – Monitored exposure to affiliated counterparties, considering their:

- creditworthiness;
- liquidity and net worth;
- track record of past performance (e.g., traded products, regulatory history, past arbitration and litigation); and
- internal risk controls.

Additional Resources

- Regulatory Notice 21-31 (FINRA Establishes New Supplemental Liquidity Schedule (SLS))
- Regulatory Notice 21-12 (FINRA Reminds Member Firms of Their Obligations Regarding Customer Order Handling, Margin Requirements and Effective Liquidity Management Practices During Extreme Market Conditions)
- FINRA’s Funding and Liquidity Topic Page

Segregation of Assets and Customer Protection

Regulatory Obligations and Related Considerations

Regulatory Obligations:

Exchange Act Rule 15c3-3 (Customer Protection Rule) imposes requirements on firms that are designed to protect customer funds and securities. Firms are obligated to maintain custody of customer securities and safeguard customer cash by segregating these assets from the firm's proprietary business activities and promptly delivering them to their owner upon request. Firms can satisfy this requirement by either keeping customer funds and securities in their physical possession or in a good control location that allows the firm to direct their movement (e.g., a clearing corporation).

Related Considerations:

- What is your firm's process to prevent, identify, research and escalate new or increased deficits that are in violation of the Customer Protection Rule?
- What controls does your firm have in place to identify and monitor its possession or control deficits, including the creation, cause and resolution?
- If your firm claims an exemption from the Customer Protection Rule and it is required to forward customer checks promptly to your firm's clearing firm, how does your firm implement consistent processes for check forwarding and maintain accurate blotters to demonstrate that checks were forwarded in a timely manner?
- How does your firm train staff on Customer Protection Rule requirements?
- What are your firm's processes to confirm that your firm correctly completes its reserve formula calculation and maintains the amounts that must be deposited into the special reserve bank account(s)?
- If your firm is engaging in digital asset transactions, what controls and procedures has it established to assure compliance with the Customer Protection Rule? Has the firm analyzed these controls and procedures to address potential concerns arising from acting as a custodian (i.e., holding or controlling customer property)?
Exam Findings and Effective Practices

Exam Findings:

- **Inconsistent Check-Forwarding Processes** – Not implementing consistent processes for check forwarding to comply with an exemption from the Customer Protection Rule.

- **Inaccurate Reserve Formula Calculations** – Failing to correctly complete reserve formula calculations due to errors in coding because of limited training and staff turnover, challenges with spreadsheet controls, limited coordination between various internal departments and gaps in reconciliation calculations.

- **Omitted or Inaccurate Blotter Information** – Maintaining blotters with insufficient information to demonstrate that checks were forwarded in a timely manner and inaccurate information about the status of checks.

Effective Practices:

- **Confirming Control Agreements** – Collaborating with legal and compliance departments to confirm that all agreements supporting control locations are finalized and executed before the accounts are established and coded as good control accounts on firms’ books and records.

- **Addressing Conflicts of Interest** – Confirming which staff have system access to establish a new good control location and that they are independent from the business areas to avoid potential conflicts of interest; and conducting ongoing review to address emerging conflicts of interest.

- **Reviews and Exception Reports for Good Control Locations** – Conducting periodic review of and implementing exception reports for existing control locations for potential miscoding, out-of-date paperwork or inactivity.

- **Check-Forwarding Procedures** – Creating and implementing policies to address receipt of customer checks, checks written to the firm and checks written to a third party.

- **Check Forwarding Blotter Review** – Creating and reviewing firms’ check received and forwarded blotters to confirm that they are up to date and include the information required to demonstrate compliance with the Customer Protection Rule exemption.

Additional Resources

- **Customer Protection – Reserves and Custody of Securities (SEA Rule 15c3-3)**


Portfolio Margin and Intraday Trading  NEW FOR 2022

Regulatory Obligations and Related Considerations

Regulatory Obligations:

FINRA Rule 4210(g) (Margin Requirements) permits member firms to apply portfolio margin requirements—based on the composite risk of a portfolio’s holdings—in margin accounts held by certain investors as an alternative to “strategy-based” margin requirements. Firms are required to monitor the risk of the positions held in these accounts during a specified range of possible market movements according to a comprehensive written risk methodology.
Related Consideration:

- Do the firm's policies and procedures for monitoring the risk of their investors' portfolio margin accounts comply with Rule 4210(g)(1), in particular:
  - maintaining a comprehensive written risk methodology for assessing the potential risk to the member's capital during a specified range of possible market movements of positions maintained in such accounts;
  - monitoring the credit risk exposure of portfolio margin accounts both intraday and end of day; and
  - maintaining a robust internal control framework reasonably designed to capture, measure, aggregate, manage, supervise and report credit risk exposure to portfolio margin accounts?

Exam Findings and Effective Practices

Exam Findings:

- **Inadequate Monitoring Systems** – Systems not designed to consistently identify credit risk exposure intra-day (e.g., do not include defined risk parameters required to produce notifications or exceptions reports to senior management; require manual intervention to run effectively) or end of day (e.g., cannot monitor transactions executed away in a timely manner).

- **Not Promptly Escalating Risk Exposures** – Staff failing to promptly identify and escalate incidents related to elevated risk exposure in portfolio margin accounts to senior management, in part due to insufficient expertise.

- **Insufficient WSPs** – Failing to maintain written supervisory procedures outlining intraday monitoring processes and controls.

Effective Practices:

- **Internal Risk Framework** – Developing and maintaining a robust internal risk framework to identify, monitor and aggregate risk exposure within individual portfolio margin accounts and across all portfolio margin accounts, including:
  - increasing house margin requirements during volatile markets in real-time;
  - conducting stress testing of client portfolios;
  - closely monitoring client fund portfolios' NAV, capital, profitability, client redemptions, liquidity, volatility and leverage to determine if higher margin requirements or management actions are required; and
  - monitoring and enforcing limits set by internal risk functions and considering trigger and termination events set forth in the agreement with each client.

- **Concentration Risk** – Maintaining and following reasonably designed processes (reflected in the firm's WSPs) and robust controls to monitor the credit exposure resulting from concentrated positions within both individual portfolio margin accounts and across all portfolio margin accounts, including processes to:
  - aggregate and monitor total exposure and liquidity risks with respect to accounts under common control;
  - identify security concentration at the aggregate and single account level; and
  - measure the impact of volatility risk at the individual security level.

- **Client Exposure** – Clearly and proactively communicating with clients with large or significantly increasing exposures, according to clearly delineated triggers and escalation channels established by the firm's WSPs; and requesting that clients provide their profit and loss position each month.

Additional Resource

- FINRA's Portfolio Margin FAQ
Appendix—Using FINRA Reports in Your Firm’s Compliance Program

Firms have used prior FINRA publications, such as Exam Findings Reports and Priorities Letters (collectively, Reports), to enhance their compliance programs. We encourage firms to consider these practices, if relevant to their business model, and continue to provide feedback on how they use FINRA publications.

- **Assessment of Applicability** – Performed a comprehensive review of the findings, observations and effective practices, and identified those that are relevant to their businesses.

- **Risk Assessment** – Incorporated the topics highlighted in our Reports into their overall risk assessment process and paid special attention to those topics as they performed their compliance program review.

- **Gap Analysis** – Conducted a gap analysis to evaluate how their compliance programs and WSPs address the questions and effective practices noted in our Reports and determined whether their compliance programs have any gaps that could lead to the types of findings noted in those Reports.

- **Project Team** – Created interdisciplinary project teams and workstreams (with staff from operations, compliance, supervision, risk, business and legal departments, among other departments) to:
  - assign compliance stakeholders and project owners;
  - summarize current policies and control structures for each topic;
  - engage the legal department for additional guidance regarding regulatory obligations;
  - develop plans to address gaps; and
  - implement effective practices that were not already part of their compliance program.

- **Circulation to Compliance Groups** – Shared copies of the publications or summaries of relevant sections with their compliance departments.

- **Presentation to Business Leaders** – Presented to business leadership about their action plans to address questions, findings, observations and effective practices from our Reports.

- **Guidance** – Used Reports to prepare newsletters, internal knowledge-sharing sites or other notices for their staff.

- **Training** – Added questions, findings, observations and effective practices from Reports, as well as additional guidance from firms’ policies and procedures, to their Firm Element and other firm training.
Endnotes

1. “Related Considerations” are intended to serve as a possible starting point in considering a firm’s compliance program related to a topic. Firms should review relevant rules to understand the full scope of their obligations.

2. “Nesting” refers to FFIs indirectly gaining access to the U.S. financial system through another FFI’s correspondent account at a U.S. financial institution. This practice can facilitate legitimate financial transactions, but member firms that maintain correspondent accounts with FFIs should have policies and procedures to identify and monitor for potentially illegitimate “nested” activity.

3. An IP address is a unique identifier assigned to an Internet-connected device, while a MAC is a unique identifier used to identify a specific hardware device at the network level.

4. See Regulatory Notice 21-18 (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts)

5. See Regulatory Notice 20-13 (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)

6. The SEC is proposing amendments to 17a-4 to allow for electronic records to be preserved in a manner that permits the recreation of an original record if it is altered, over-written, or erased. See the SEC’s Proposed Rule: Electronic Recordkeeping Requirements for Broker-Dealers, Security-Based Swap Dealers, and Major Security-Based Swap Participants.

7. These regulatory obligations stem from Exchange Act Rule 15c3-3(d)(4) and MSRB Rules G-17 and G-27 (for firm shorts), and MSRB Rule G12(h) (for fails-to-receive).

8. Reg BI also applies to certain recommendations that were not previously covered under suitability obligations (e.g., account recommendations, implicit hold recommendations in the case of agreed-upon account monitoring).

9. When a retail customer opens or has an existing account with a broker-dealer, the retail customer has a relationship with the broker-dealer and is therefore in a position to “use” the broker-dealer’s recommendation.

10. While the SEC presumes that the use of the term “adviser” or “advisor” in a name or title by an associated person of a broker-dealer who is not also a supervised person of an investment adviser is a violation of the Disclosure Obligation under Reg BI, it recognizes that usage may be appropriate under certain circumstances. See FINRA’s Reg BI and Form CRS Checklist for examples of possible exceptions.

11. See the SEC’s December 17, 2021 Staff Statement Regarding Form CRS Disclosures for additional observations.

12. Regulatory Notice 21-10 summarized the recent updates to the 5122/5123 Notification Filing Form that became effective on May 22, 2021, and Regulatory Notice 21-26 announced that, as of October 1, 2021, FINRA Rules 5122 and 5123 require member firms to file retail communications that promote or recommend a private placement offering that is subject to these rules’ filing requirements with FINRA’s Corporate Financing Department.

13. See CAT NMS Plan, FAQ R.2 for the types of information firms should obtain from third-party vendors to satisfy these requirements.


15. In addition to the order routing disclosures under Rule 606, Rule 607 of Regulation NMS requires firms to disclose their policies regarding PFOF and order routing when customers open accounts, and on an annual basis thereafter, so firms should consistently provide the same information in both types of disclosures.

16. Firms are reminded that any affiliate obligated to pay firm expenses must have the independent financial means to satisfy those obligations.
Introduction

This Report on FINRA’s Risk Monitoring and Examination Activities (the Report) is designed to inform member firms’ compliance programs by providing annual insights from FINRA’s ongoing regulatory operations. For selected regulatory obligations, the Report: (1) identifies the applicable rule and key related considerations for member firm compliance programs; (2) summarizes noteworthy findings from recent examinations and outlines effective practices that FINRA observed during its oversight; and (3) provides additional resources that may be helpful to member firms.

The Report replaces two of FINRA’s prior publications: (1) the Report on FINRA Examination Findings and Observations, which provided an analysis of prior examination results; and (2) the Risk Monitoring and Examination Priorities Letter, which highlighted areas we planned to review in the coming year.

FINRA expects to revisit the Report annually, as we did with these prior publications. Many of the areas addressed in the Report represent ongoing core compliance responsibilities that are reviewed as part of our risk-based exam program each year. Where applicable, we will continue to evolve the information in these areas to address changes in business models, technologies, compliance practices and other factors that may affect how regulatory obligations are fulfilled. Other areas addressed in the Report may be episodic or tied to a particular development, such as a new regulatory requirement or investment product. We expect to include these areas during the periods when they may be most relevant for member firms’ compliance programs.

FINRA welcomes feedback on how we can improve future publications of this Report. Please contact Ursula Clay, Senior Vice President, Member Supervision at (646) 315-7375 or by email; or Elena Schlickenmaier, Senior Principal Analyst, Member Supervision, at (202) 728-6920 or by email.

Firms’ Practices During COVID-19

In Regulatory Notice 20-16 (FINRA Shares Practices Implemented by Firms to Transition to, and Supervise in, a Remote Work Environment During the COVID-19 Pandemic), we shared common themes FINRA noted through discussions with firms about the steps they reported taking in response to the pandemic and in connection with their move to remote work environments. This Report does not address exam findings, observations or effective practices specifically relating to how firms adjusted their operations during the pandemic. Those reviews are underway now and will be addressed in a future publication.
Selected Highlights

This Report addresses several regulatory key topics for each of the four categories: (1) Firm Operations; (2) Communications and Sales; (3) Market Integrity; and (4) Financial Management. As described further in the “How to Use This Report” section below, the importance and relevance of the considerations, findings and effective practices in each of these areas will vary for each member firm.

In general, however, there are several key areas to highlight that impact compliance programs across a large population of member firms:

► **Regulation Best Interest (Reg BI) and Form CRS** — We will continue to focus on assessing whether member firms have established and implemented policies, procedures, and a system of supervision reasonably designed to comply with Reg BI and Form CRS. However, in 2021, we intend to expand the scope of our Reg BI and Form CRS reviews and testing to effect a more comprehensive review of firm processes, practices and conduct. As always, FINRA will take appropriate action in the event we observe conduct that may cause customer harm, would have violated previous standards (e.g., suitability), or indicates a clear disregard of the requirements of Reg BI and Form CRS. In the Reg BI and Form CRS section below, member firms should review considerations our staff will use when examining a firm for compliance with Reg BI and Form CRS. The Report also includes a list of previously published considerations and materials—such as our Reg BI Topic Page.

► **Consolidated Audit Trail (CAT)** — As we noted in *Regulatory Notice 20-31* (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT), all member firms that receive or originate orders in National Market System (NMS) stocks, over-the-counter (OTC) equity securities or listed options must report to CAT. All proprietary trading activity, including market making activity, is subject to CAT reporting. There are no exclusions or exemptions for size or type of firm or type of trading activity. FINRA is in the early stages of reviewing for compliance with certain CAT obligations; accordingly, exam findings or effective practices are not included in this Report but will be provided later when more information is available. In the interim, member firms should review the list of recommended steps provided in the Notice and the list of considerations and relevant resources provided in this Report in assessing the adequacy of their CAT compliance programs.

► **Cybersecurity** — Member firms’ ongoing and increasing reliance on technology for many customer-facing activities, communications, trading, operations, back-office and compliance programs—especially in our current remote work environment—requires them to address new and existing cybersecurity risks, including risks relating to cybersecurity-enabled fraud and crime. A firm’s cybersecurity program should be reasonably designed and tailored to the firm’s risk profile, business model and scale of operations. FINRA reminds firms that we review cybersecurity programs for compliance with business continuity plan requirements, as well as the SEC’s Regulation S-P Rule 30, which requires member firms to have policies and procedures addressing the protection of customer records and information. Given the increase in remote work and virtual client interactions, combined with an increase in cyber-related crimes, we encourage member firms to review the considerations, observations and effective practices noted in the Report, as well as *Regulatory Notice 20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic), *Report on Selected Cybersecurity Practices – 2018* and *Report on Cybersecurity Practices – 2015*.

► **Communications with the Public** — FINRA continues to evaluate member firms for compliance with FINRA Rule 2210 (Communications with the Public), which includes principles-based content standards that are designed to apply to ongoing developments in communications technology and practices. In addition, we are increasingly focused on communications relating to certain new products, and how member firms supervise, comply with recordkeeping obligations, and address risks relating to new digital communication channels. This focus includes risks associated with app-based platforms with interactive or “game-like” features that are intended to influence customers, their related forms of marketing, and the appropriateness of the activity that they are approving clients to undertake through those platforms (e.g., under FINRA Rule 2360 (Options)). The Report also addresses the communications relating to cash management services that sweep customer cash into affiliate or partner
banks or money market funds (Cash Management Accounts). As always, we remain focused on reviewing member firms’ communications relating to complex products, as well as the information firms convey to senior and vulnerable investors.

**Best Execution** – FINRA has routinely reviewed member firms for their compliance with best execution obligations under FINRA Rule 5310 (Best Execution and Interpositioning) in our examinations. Among other things, FINRA has continued to focus on potential conflicts of interest in order-routing decisions, appropriate policies and procedures for different order and security types, and the sufficiency of member firms’ reviews of execution quality. We also conducted a targeted review of member firms that do not charge commissions for customer transactions (“zero commission” trading) to evaluate the impact that not charging commissions has or will have on member firms’ order-routing practices and decisions, and other aspects of member firms’ business. In addition to general compliance considerations, findings and effective practices from our examination program, the Report also includes themes we noted in the “zero commission” targeted review.

**Variable Annuities** – FINRA continues to evaluate variable annuity exchanges under FINRA Rule 2330 (Members’ Responsibilities Regarding Deferred Variable Annuities) and, when applicable, under Reg BI. Additionally, in early 2020, we engaged in an informal review of buyout written supervisory procedures (WSPs), training, and disclosures for member firms whose customers were impacted by a recent announcement from an insurer with sizable variable annuity assets stating it will terminate servicing agreements, cancel certain trail commissions for registered representatives, and provide buyout offers to its variable annuity customers. In addition to reviewing considerations and findings provided in the Report, we encourage member firms to consider the effective practices we identified as part of this particular review.

**How to Use the Report**

FINRA’s Risk Monitoring and Examination Programs evaluate member firms for compliance with relevant obligations and consider specific risks relating to each firm, including those relating to a firm’s business model, supervisory control system and prior exam findings, among other considerations. While the topics addressed in this Report are selected for their interest to the largest number of member firms, they may include areas that are not relevant to an individual member firm and omit other areas that are applicable.

FINRA advises each member firm to review the Report and consider incorporating relevant practices into its compliance programs in a manner tailored to its activities. The Report is intended to be just one of the tools a member firm can use to help inform the development and operation of its compliance program; it does not represent a complete inventory of regulatory obligations, compliance considerations, examination findings, effective practices or topics that FINRA will examine.

FINRA also reminds member firms to stay apprised of new or amended laws, rules and regulations, and to update their WSPs and compliance programs on an ongoing basis, as new regulatory obligations may be part of future examinations. FINRA encourages member firms to reach out to their designated Risk Monitoring Analyst if they have any questions about the considerations, findings and effective practices described in this Report.

Each area of regulatory obligations is set forth as follows:

**Regulatory Obligations and Related Considerations** – A brief description of:

- relevant federal securities laws, regulations and FINRA rules; and
- questions FINRA may ask or consider when examining your firm for compliance with such obligations. We encourage member firms to use these questions, if applicable, when evaluating their compliance programs and related controls, and preparing for FINRA examinations.
Exam Findings and Effective Practices

- Noteworthy findings that FINRA has noted at some—but not all—member firms, including:
  - new findings from recent examinations;
  - findings we highlighted in the 2017, 2018 and 2019 Exam Findings Reports, and continue to note in recent examinations;
  - in certain sections, topics noted as “Emerging Risks” representing potentially concerning practices that FINRA has observed and which may receive increased scrutiny going forward; and
  - for certain topics, such as Cybersecurity, Liquidity Management and Credit Risk, observations that suggested improvements to a firm’s control environment to address potential weaknesses that elevate risk, but for which there are not specific rule violations.

- Select effective practices FINRA observed in recent exams, as well as those we noted in prior Exam Findings Reports and which we continue to see, that may help member firms, depending on their business model, evaluate their own programs.

Supervision

We do not address supervisory deficiencies or practices in a separate Supervision topic, but rather, address them as part of the underlying regulatory obligation (e.g., supervisory shortcomings relating to annuity exchanges are addressed in the Variable Annuities section).

Senior and Vulnerable Investors

We also do not include a separate section on senior or vulnerable investors because FINRA considers such investors when evaluating firms’ compliance programs for many of the topics addressed in this Report, including determining the egregiousness of an exam finding or rule violation. FINRA remains highly focused on, and committed to, protecting senior and vulnerable investors, and takes this into consideration when evaluating communications, recommendations of certain products, and sales practice conduct.

Additional Resources

- A list of relevant FINRA Notices, other reports, tools and online resources.

The Report also includes an Appendix that outlines how member firms have used similar FINRA reports (Exam Findings Reports or Priorities Letters) in their compliance programs.

As a reminder, the Report—like our previous Exam Findings Reports and Priorities Letters—does not create any new legal or regulatory requirements or new interpretations of existing requirements. You should not infer that FINRA requires member firms to implement any specific practices described in this report extend beyond the requirements of existing federal securities rules and regulations or FINRA rules.
Firm Operations

Anti-Money Laundering

Regulatory Obligations and Related Considerations

Regulatory Obligations

The Bank Secrecy Act (BSA) requires firms to monitor for, detect and report suspicious activity conducted or attempted by, at, or through the firms to the U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN). Firms should also be aware of the recently enacted Anti-Money Laundering Act of 2020, which may result in material revisions to the implementing regulations over time.

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires that members develop and implement a written anti-money laundering (AML) program reasonably designed to comply with the requirements of the BSA and its implementing regulations. Additionally, FinCEN’s Customer Due Diligence (CDD) rule requires that firms identify beneficial owners of legal entity customers, understand the nature and purpose of customer accounts, and conduct ongoing monitoring of customer accounts to identify and report suspicious transactions and—on a risk basis—update customer information.

Related Considerations

- How does your firm’s AML compliance program address new business lines, products, customers and risks?
- Does your firm tailor and adequately resource their AML program to the firm’s business model and associated AML risks?
- Does your firm’s independent testing confirm that it maintains appropriate risk-based procedures for collecting and verifying customer identification information on all individuals and entities that would be considered customers under the Customer Identification Program rule, and beneficial owners of legal entity customers under the CDD rule?
- Does your firm review the integrity of its data feeds for its surveillance and monitoring programs?
- How does your firm coordinate with your clearing firm, including with respect to the filing of joint suspicious activity reports?
- Does your firm document the results of its reviews and investigations into potentially suspicious activity identified by exception reports?

Exam Findings and Effective Practices

Exam Findings

- Inadequate AML Transaction Monitoring – Not tailoring transaction monitoring to address firms’ business risk(s).
- Limited Scope for Suspicious Activity Reports (SARs) – Not requiring staff to notify AML departments or file SARs for a range of events involving suspicious transactions, such as financial crime-related events, including but not limited to cybersecurity events, account compromises, account takeovers, new account fraud and fraudulent wires.
Inadequate AML Framework for Cash Management Accounts – Failing to incorporate, or account for, in their AML programs, the AML risks relating to Cash Management Accounts, including the following:

- monitoring, investigating and reporting suspicious money movements;
- a list of red flags in their WSPs indicative of potentially suspicious transactions; or
- expanding or enhancing their AML compliance program resources to address Cash Management Accounts.

Unclear Delegation of AML Responsibilities – Non-AML staff (e.g., business line staff responsible for trade surveillance) failing to escalate suspicious activity monitoring alerts to AML departments because firms did not: (1) clearly define the activities that were being delegated; (2) articulate those delegations and related surveillance responsibilities in their WSPs; or (3) train non-AML staff on AML surveillance policies and procedures.

Data Integrity Gaps – Excluding certain types of data and customer accounts from monitoring programs as a result of problems with ingesting certain data, inaccuracies and missing information in data feeds.

Failure to Document Investigations – Not documenting initial reviews and investigations into potentially suspicious activities identified by SARs.

Concerns About High-Risk Trading by Foreign Legal Entity Accounts – Inadequate identification of or follow-up on increased trading by foreign legal entity accounts in similar low-float and low-priced securities, which raised concerns about potential ownership or control by similar beneficial owners.

Insufficient Independent Testing – Not reviewing how the firm’s AML program was implemented; not ensuring independence of the testing; and not completing tests on an annual calendar year basis.

Improper Reliance on Clearing Firms – Introducing firms relying primarily or entirely on their clearing firms for transaction monitoring and suspicious activity reporting, even though they are required to monitor for suspicious activity attempted or conducted through their firms.
Emerging AML and Other Financial Crime Risks

Microcap and Other Fraud

Some firms continue to engage in fraud, financial crimes and other problematic practices, such as those described in the SEC Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities, which addresses microcap and penny stock activity transacted in omnibus accounts maintained for foreign financial institutions and foreign affiliates of U.S. broker-dealers.

Issuers Based in Restricted Markets

Certain foreign national and foreign entity nominee accounts appear to have been opened solely to invest in the initial public offerings and subsequent aftermarket trading in one or more exchange-listed issuers based in restricted markets, such as China. FINRA has observed red flags that the owners of the accounts may be acting at the direction of others, multiple accounts being opened using the same foreign bank for the source of funds or multiple accounts with the same employer and same email domain. The trading activity may include multiple similar limit orders being placed by the accounts at the same time, which could be indicative of coordinated and manipulative trading of the issuers’ securities.

Risks Relating to Special Purpose Acquisition Companies (SPACs)

Some firms are engaging in the formation and initial public offerings (IPOs) of SPACs without having adequate WSPs that would require independently conducting due diligence of SPACs’ sponsors, and procedures that address other potential fraud risks, including but not limited to:

- misrepresentations and omissions in offerings documents and communications with shareholders regarding SPAC acquisition targets, such as the prospects of the target company and its financial condition;
- fees associated with SPAC transactions, including cash and non-cash compensation and compensation earned by affiliates;
- control of funds raised in SPAC offerings; and
- insider trading (where underwriters and SPAC sponsors may possess and trade around material non-public information regarding potential SPAC acquisition targets, including private placement offerings with rights of first refusal provided to certain investors prior to the acquisition).

Effective Practices

- **Customer Identification Program** – Using, on a risk-basis, both documentary (such as drivers’ licenses or passports) and non-documentary methods (such as using third-party sources) to verify customers’ identities.

- **Monitoring for Fraud During Account Opening** – Implementing additional precautions during account opening, including limiting automated approval of multiple accounts opened by a single customer; reviewing account application fields for repetition or commonalities among multiple applications; and using technology to detect indicators of automated scripted attacks in the digital account application process.

- **Bank Account Verification, Restrictions on Fund Transfers and Ongoing Monitoring** – Confirming customers’ identities through verbal confirmation, following client verification protocols or using a third-party verification service, such as Early Warning System (EWS); monitoring of outbound money movement requests post-ACH set-up; restricting fund transfers in certain situations; and conducting ongoing monitoring of accounts.

- **Collaboration With Clearing Firms** – Understanding the allocation of responsibilities between clearing and introducing firms for handling ACH transactions; and implementing policies and procedures to comply with those responsibilities.
AML Compliance Tests — Confirming annual AML independent tests evaluate the adequacy of firms’ AML compliance programs, review firms’ SAR reporting processes, and include sampling and transaction testing of firms’ monitoring programs.

Risk Assessments — Updating risk assessments based on the results of AML independent tests, audits, and changes in size or risk profile of the firms, including their businesses, registered representatives and customer account types; and using AML risk assessments to inform the focus of firms’ independent AML tests.

Testing of Transaction Monitoring and Model Validation — Performing regular, ongoing testing and tuning of transaction monitoring models, scenarios and thresholds; and confirming the integrity of transaction monitoring data feeds and validating models (which are more frequently used at large firms).

Collaboration with AML Department — Increasing the likelihood that all potentially reportable events are referred to the AML department by establishing a line of communication (such as reporting and escalation processes, awareness and educational programs, regular meetings, policies and procedures, or exception reports) between the AML department and other departments that may observe potentially reportable events (such as registered representatives and client-facing teams, technology, cybersecurity, compliance, operations, trading desks and fraud departments).

Training Programs — Designing training programs for each of the roles and responsibilities of the AML department (as well as departments that regularly work with AML) and addressing all AML regulatory and industry developments.

Additional Resources

- Regulatory Notice 20-13 (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- Regulatory Notice 19-18 (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)
- SEC Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities
- Anti-Money Laundering (AML) Template for Small Firms
- Frequently Asked Questions (FAQ) Regarding Anti-Money Laundering (AML)
- Anti-Money Laundering (AML) Topic Page

Cybersecurity and Technology Governance

Regulatory Obligations and Related Considerations

Regulatory Obligations

The SEC’s Regulation S-P Rule 30 requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members’ operations. In addition to firms’ compliance with SEC regulations, FINRA reminds firms that cybersecurity remains one of the principal operational risks facing broker-dealers, and expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

Technology-related problems, such as problems in firms’ change- and problem-management practices, can expose firms to operational failures that may compromise firms’ ability to comply with a range of rules and regulations, including FINRA Rules 4370 (Business Continuity Plans and Emergency Contact Information), 3110 (Supervision) and 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.
Related Considerations

- What kind of governance structure has your firm developed to identify and respond to cybersecurity risks?
- What is the scope of your firm’s Data Loss Prevention program, including encryption controls?
- How does your firm address branch-specific cybersecurity risks?
- What kind of training does your firm conduct on cybersecurity, including phishing?
- What process does your firm have to evaluate your firm’s vendors’ cybersecurity controls?
- Has your firm implemented multi-factor authentication (MFA) or other relevant access management controls?
- What controls does your firm implement to mitigate system capacity performance and integrity issues that may undermine its ability to conduct business and operations, monitor risk or report key information?
- How does your firm document system change requests and approvals?
- What type of testing does your firm perform prior to changes being moved into a production environment and post-implementation?
- What are your firm’s procedures for tracking information technology problems and their remediation? Does your firm categorize problems based on their business impact?

Exam Observations and Effective Practices

Exam Observations

- **Data Loss Prevention Programs** – Not encrypting all confidential data, including a broad range of non-public customer information in addition to Social Security numbers (such as other account profile information and firm information).
- **Branch Policies, Controls and Inspections** – Not maintaining branch-level written cybersecurity policies; inventories of branch-level data, software and hardware assets; and branch-level inspection and automated monitoring programs.
- **Training** – Not providing comprehensive training to registered representatives, personnel, third-party providers and consultants on cybersecurity risks relevant to individuals’ roles and responsibilities, including phishing.
- **Vendor Controls** – Not implementing and documenting formal policies and procedures to review prospective and existing vendors’ cybersecurity controls and managing the lifecycle of firms’ engagement with all vendors (i.e., from onboarding, to ongoing monitoring, through off-boarding, including defining how vendors will dispose of non-public client information).
- **Access Management** – Not implementing access controls, including developing a “policy of least privilege” to grant system and data access only when required and removing it when no longer needed; not limiting and tracking individuals with administrator access; and not implementing MFA for registered representatives, employees, vendors and contractors.
- **Inadequate Change Management Supervision** – Insufficient supervisory oversight for application and technology changes (including upgrades, modifications to or integration of firm or vendor systems), which lead to violations of other regulatory obligations, such as those relating to data integrity, cybersecurity, books and records, and confirmations.
- **Limited Testing and System Capacity** – Order management system, account access and trading algorithm malfunctions due to a lack of testing for changes or system capacity issues.
Emerging Cybersecurity Risks
FINRA recently observed increased numbers of cybersecurity- or technology-related incidents at firms, including:

- systemwide outages;
- email and account takeovers;
- fraudulent wire requests;
- imposter websites; and
- ransomware.

We also noted data breaches at some firms and remain concerned about increased risks for firms that do not implement practices to address phishing emails or require MFA for accessing non-public information.

We remind firms to review the practices noted below, as well as the materials noted in the associated Additional Resources section.

Effective Practices

- **Insider Threat and Risk Management** – Collaborating across technology, risk, compliance, fraud, and internal investigations/conduct departments to assess key risk areas, monitor access and entitlements, and investigate potential violations of firm rules or policies with regard to data access or data accumulation.

- **Incident Response Planning** – Establishing and regularly testing written formal incident response plans that outlined procedures for responding to cybersecurity and information security incidents; and developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents.

- **System Patching** – Implementing timely application of system security patches to critical firm resources (e.g., servers, network routers, desktops, laptops and software systems) to protect non-public client or firm information.

- **Asset Inventory** – Creating and keeping current an inventory of critical information technology assets—including hardware, software and data—as well as corresponding cybersecurity controls.

- **Change Management Processes** – Implementing change management procedures to document, review, prioritize, test, approve, and manage hardware and software changes, as well as system capacity, in order to protect non-public information and firm services.

Additional Resources

- **Regulatory Notice 20-32** (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud)

- **Information Notice 03/26/20** (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19))

- **Regulatory Notice 20-13** (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)


- **Small Firm Cybersecurity Checklist**

- **Core Cybersecurity Controls for Small Firms**

- **Customer Information Protection Topic Page**

- **Cybersecurity Topic Page**

- **Non-FINRA Cybersecurity Resources**
Outside Business Activities and Private Securities Transactions

Regulatory Obligations and Related Considerations

Regulatory Obligations

FINRA Rules 3270 (Outside Business Activities of Registered Persons) and 3280 (Private Securities Transactions of an Associated Person) require registered representatives to notify their firms in writing of proposed outside business activities (OBAs), and all associated persons to notify their firms in writing of proposed private securities transactions (PSTs), so firms can determine whether to limit or allow those activities. A firm approving a PST where the associated person has or may receive selling compensation must record and supervise the transaction as if it were executed on behalf of the firm.

Related Considerations

- Do your firm’s WSPs explicitly state where notification or pre-approval is required to engage in an OBA or PST?
- Does your firm require associated persons or registered persons to complete and update, as needed, questionnaires and attestations regarding their involvement—or potential involvement—in OBAs and PSTs; and if yes, how often?
- Do you have a process in place in to update a registered representative’s Form U4 with OBAs that meet the disclosure requirements of that form?
- What methods does your firm use to identify individuals involved in undisclosed OBAs and PSTs?
- Does your firm take into account the unique regulatory considerations and characteristics of digital assets when reviewing digital asset OBAs and PSTs?
- How does your firm supervise PSTs, including digital asset PSTs, and document its compliance with the supervisory obligations?
- Does your firm record the PSTs on its books and records, including PSTs involving new or unique products and services?

Exam Findings and Effective Practices

Exam Findings

- Incorrect Interpretation of Requirements – Interpreting “compensation” too narrowly (by focusing on only direct compensation, such as salary or commissions, rather than evaluating all direct and indirect financial benefits from PSTs, such as membership interests, receipt of preferred stock and tax benefits); and, as a result, erroneously determining that certain activities were not PSTs, or approving participation in proposed transactions without adequately considering whether the firms need to supervise the transaction as if it were executed on their own behalf.
- No Documentation – Not retaining the documentation necessary to demonstrate firms’ compliance with the supervisory obligations for PSTs and not recording the transactions on the firm’s books and records because certain PSTs were not consistent with firms’ electronic systems (such as where securities businesses conducted by a registered representative would not be captured in their clearing firm’s feed of purchases and sales activity).
- No or Insufficient Notice and Notice Reviews – Registered persons failing to notify their firms in writing of OBAs or PSTs; and WSPs not requiring the review of such notices, or the documentation that such reviews had taken place.
No PST Monitoring – Not monitoring limitations placed on OBAs or PSTs, such as prohibiting registered representatives from soliciting firm clients to participate in the OBA or PST.

No Review and Recordkeeping of Digital Asset Activities – Incorrectly assuming all digital assets are not securities and, therefore, not evaluating digital asset activities, including activities performed by affiliates, to determine whether they are PSTs; and for certain digital asset or other activities that were deemed to be PSTs because registered representatives received selling compensation, not supervising such activities or recording such transactions on the firm’s books and records.

Emerging OBA/PST Risks
Paycheck Protection Program (PPP) Loans for Registered Representatives

FINRA noted that some registered representatives received a PPP loan for an OBA that had not been disclosed to their firms, and which may have required an update to their Form U4 as well. Firms should consider reviewing the publicly available data on PPP loans to determine if they have a registered representative who obtained a PPP loan for an undisclosed OBA.

Effective Practices

Questionnaires – Requiring registered representatives and other associated persons to complete upon hire, and periodically thereafter, detailed, open-ended questionnaires with regular attestations regarding their involvement—or potential involvement—in new or previously disclosed OBAs and PSTs (including asking questions relating to any other businesses where they are owners or employees; whether they are raising money for any outside activity; whether they act as “finders”; and any expected revenues or other payments they receive from any entities other than member firms, including affiliates).

Thorough Reviews – Conducting reviews to learn about all OBAs and PSTs at the time of a registered representative’s initial disclosure to the firm and periodically thereafter, including thorough reviews of:

- social media, professional networking and other publicly available websites and other sources (such as legal research databases and court records);
- email, social media and other communications;
- interviews with registered representatives; and
- documentation supporting the activity (such as organizational documents).

Monitoring – Monitoring significant changes in or other red flags relating to registered representatives’ or associated persons’ performance, production levels, or lifestyle that may indicate involvement in undisclosed or prohibited OBAs and PSTs (or other business or financial arrangements with their customers, such as borrowing or lending), including conducting regular, periodic background checks and reviews of:

- correspondence (including social media);
- fund movements;
- marketing materials;
- online activities;
- customer complaints; and
- financial records (including bank statements and tax returns).
- **Affiliate Activities** – Considering whether registered representatives’ and other associated persons’ activities with affiliates, especially self-offerings, may implicate FINRA Rules 3270 and 3280.
- **WSPs** – Clearly identifying types of activities or investments that would constitute an OBA or PST subject to disclosure/approval or not, as well as defining compensation, and in some cases, providing FAQs to remind employees of scenarios that they might not otherwise consider applicable to these rules.
- **Training** – Conducting training on OBAs and PSTs during onboarding and periodically thereafter, including regular reminders that registered representatives must give written notice of such activities to their firms and update their disclosures.
- **Disciplinary Action** – Imposing significant consequences—including heightened supervision, fines or termination—for registered representatives and associated persons who fail to notify firms in writing and receive approval for their OBAs and PSTs.
- **Digital Asset Checklists** – Creating checklists with a list of considerations to confirm whether digital asset activities would be considered OBAs or PSTs (including reviewing private placement memoranda or other materials and analyzing the underlying products and investment vehicle structures).

### Additional Resources
- *Regulatory Notice 20-23* (FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- *Notice to Members 96-33* (NASD Clarifies Rules Governing RRs/IAs)
- *Notice to Members 94-44* (Board Approves Clarification on Applicability of Article III, Section 40 of Rules of Fair Practice to Investment Advisory Activities of Registered Representatives)

### Books and Records

#### Regulatory Obligations and Related Considerations

**Regulatory Obligations**

Exchange Act Rules 17a-3 and 17a-4, as well as FINRA Rule 3110(b)(4) (Review of Correspondence and Internal Communications) and FINRA Rule Series 4510 (Books and Records Requirements) (collectively, Books and Records Rules) require a firm to, among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to its “business as such.”

Such records must be immediately produced or reproduced and may be maintained and preserved for the required time on electronic storage media (ESM) subject to the conditions set forth in Exchange Act Rule 17a-4(f)(2) (ESM Standards), including “non-rewriteable and non-erasable format.” Firms must also provide notification to FINRA as required by Exchange Act Rule 17a-4(f)(2)(i), including a representation that the selected storage media meets the conditions of Exchange Act Rule 17a-4(f)(2) and a third-party attestation as set forth in Exchange Act Rule 17a-4(f)(3)(vii) (collectively, ESM Notification Requirements).
Related Considerations

▶ What kind of vendors, such as cloud service providers (Cloud Vendors), does your firm use to comply with Books and Records Rule requirements, including storing required records on ESM? How does it confirm compliance with the Books and Records Rules, ESM Standards and ESM Notification Requirements?

▶ Has your firm reviewed its Books and Records Rule policies and procedures to confirm they address all vendors, including Cloud Vendors?

Exam Findings and Effective Practices

Exam Findings

▶ Misinterpreted Obligations – Not performing due diligence to verify vendors’ ability to comply with Books and Records Rules requirements if they use that vendor; or not confirming that service contracts and agreements comply with ESM Notification Requirements, because they did not understand that all required records must comply with the Books and Records Rules, including records stored using Cloud Vendors’ storage services.

▶ No ESM Notification – Not complying with the ESM Notification Requirements, including obtaining the third-party attestation letters required by Exchange Act Rule 17a-4(f)(3)(vii).

Effective Practices

▶ Contract Review – Reviewing vendors’ contracts and agreements to assess whether firms will be able to comply with the Books and Records Rules, ESM Standards and ESM Notification Requirements.

▶ Testing and Verification – Testing all vendors’—including Cloud Vendors’—capabilities to fulfill regulatory obligations by, for example, simulating a regulator’s examinations by requesting records, and engaging regulatory or compliance consultants to confirm compliance with the Books and Records Rule, ESM Standards and ESM Notification Requirements (and, in some cases, engaging the consultant to provide the third-party attestation).

▶ Attestation Verification – Confirming with vendors, including Cloud Vendors, whether the firms or the vendors will provide the third-party attestation.

Additional Resources


▶ Books and Records Requirements Checklist

▶ Books and Records Topic Page

Regulatory Events Reporting

Regulatory Obligations and Related Considerations

Regulatory Obligations

FINRA Rule 4530 (Reporting Requirements) requires firms to promptly report to FINRA, and associated persons to promptly report to firms, specified events, including, for example, violations of securities laws and FINRA rules, certain written customer complaints and certain disciplinary actions taken by the firm. Firms must also report quarterly to FINRA statistical and summary information regarding certain written customer complaints.
Related Considerations

- Do your firm’s WSPs require associated persons to report written customer complaints, judgments, liens and other events to the firm’s compliance department?
- Does your firm provide periodic reminders or training on such requirements, and what consequences does your firm impose on those persons that do not comply?
- How does your firm monitor for red flags of unreported written customer complaints and other reportable events?
- How does your firm ensure that it accurately and timely reports to FINRA written customer complaints that associated persons reported to your firm’s compliance department?
- How does your firm determine the problem and product codes it uses for its statistical reporting of written customer complaints to FINRA?

Exam Findings and Effective Practices

Exam Findings

- No Reporting to the Firm – Associated persons not reporting complaints, judgments, liens and other events to the firms’ compliance departments because they were not aware of firm requirements;
- Inadequate Surveillance – Firms not conducting regular email and other surveillance for unreported events.
- No Reporting to FINRA – Failing to report to FINRA written customer complaints that associated persons reported to the firms’ compliance departments.
- Incorrect Rule 4530 Product/Problem Codes – As part of the statistical reporting to FINRA, failing to use codes that correlated to the most prominent product or the most egregious problem alleged in the written customer complaints, but instead, reporting less prominent or severe codes or other codes based on the firms’ investigations or other information.

Effective Practices

- Compliance Questionnaires – Developing detailed annual compliance questionnaires to verify the accuracy of associated persons’ disclosures, including follow-up questions (such as whether they have ever filed for bankruptcy, have any pending lawsuits, are subject to an unsatisfied judgments or liens, or received any written customer complaints).
- Email Surveillance – Conducting email surveillance targeted to identify unreported complaints (by, for example, including complaint-related words in their keyword lexicons, reviewing for unknown email addresses, and conducting random email checks).
- Review of Registered Representatives’ Financial Condition – Identifying expenses, settlements and other payments that may indicate unreported events by conducting periodic reviews of their associated persons’ financial condition, including background checks and credit reports.
- Review of Publicly Available Information – Conducting periodic searches of associated persons’ names on web forums, court filings and other publicly available databases, including reviewing for any judgments, liens and other reportable events.
Fixed Income Mark-up Disclosure

Regulatory Obligations and Related Considerations

Regulatory Obligations

Since 2018, FINRA’s and the Municipal Securities Rulemaking Board’s (MSRB) amendments to FINRA Rule 2232 (Customer Confirmations) and MSRB Rule G-15 have required firms to provide additional transaction-related information to retail customers for certain trades in corporate, agency and municipal debt securities (other than municipal fund securities). Disclosed mark-ups and mark-downs must be expressed as both a total dollar amount for the transaction and a percentage of prevailing market price (PMP). In addition, for all retail customer trades in corporate, agency and municipal debt securities (other than municipal fund securities), firms must disclose on the confirmation the time of execution and a security-specific link to the FINRA or MSRB website where additional information about the transaction is available, along with a brief description of the information available on the website.

Related Considerations

- What are the frequency, scope and depth of your firm’s review of the accuracy of your firm’s confirmations, and does it include reviewing samples of confirmations?
- How does your firm work with its clearing firm(s) to ensure the accuracy of your firm’s confirmations?
- Is the process to ensure mark-up disclosures appear on confirmations manual or automated?
- What is the scope of diligence and oversight your firm conducts on customer confirmation vendors?
- Has your firm considered how to maintain consistent and correct disclosures for fixed income transactions executed across different vendors, platforms or trading desks?
Exam Findings and Effective Practices

Exam Findings

► **Incorrect PMP Determinations** — Adjusting the PMP in firms’ order entry systems to subtract registered representatives’ concession or sales credit from the mark-up; PMP not presumptively relying on the dealer’s contemporaneous cost or proceeds; deciding that firms’ costs or proceeds were no longer “contemporaneous” without sufficient evidence as required by FINRA Rule 2121.02(b)(4) and using other pricing information to determine the PMP.

► **Incorrect Compensation Disclosures** — Disclosing additional charges separately from disclosed mark-ups or mark-downs, even when such charges reflected firm compensation; disclosing registered representatives’ sales credits or concessions as separate line items on confirmations, in addition to the mark-up or mark-down, without clear and accurate labeling; inaccurately labeling only the sales credits or concessions portion as the total mark-up or mark-down.

► **Failure to Provide Accurate Time of Execution** — Disclosing times of execution on customer confirmations that did not match the times of execution disseminated by the Electronic Municipal Market Access system (EMMA) or Trade Reporting and Compliance Engine (TRACE).

► **Disclosure for Structured Notes** — Failing to provide disclosures on customer confirmations for trades in TRACE-reportable structured notes because firms did not realize the notes were subject to FINRA Rule 2232 or did not receive the PMP from the structured note distributors.

► **Incorrect Designation of Institutional Accounts** — Failing to provide disclosures to certain customers because the firm identified those customers’ accounts as “institutional,” even though the customers did not meet the “institutional” definition in FINRA Rule 4512(c) (Customer Account Information) or MSRB Rule G-8(a)(xi).

Effective Practices

► **Confirmation Review** — Performing regular reviews of confirmations, including samples of confirmations, to confirm the accuracy of all disclosures, including all of the required disclosure elements, including the mark-up or mark-down, the time of execution and the security-specific link (with CUSIP).

► **Collaborating With Clearing Firms** — For correspondent firms, engaging with clearing firms to understand their policies and processes for providing mark-up disclosure.

► **Due Diligence of Vendors** — Conducting due diligence into customer confirmation vendors’ processes and methodology to determine PMP.

► **Product and Customer Review** — Reviewing firm confirmation systems and processes to confirm that they cover all products and customers subject to FINRA Rule 2232 (in particular, whether they accurately categorize “institutional” customers using the definition in FINRA Rule 4512(c) or MSRB Rule G-8(a)(xi)).

Additional Resources


► **Report Center** — FINRA’s MSRB Markup/Markdown Analysis Report

► **Report Center** — FINRA’s TRACE Markup/Markdown Analysis Report

► **Fixed Income Confirmation Disclosure: Frequently Asked Questions (FAQ)**

► **Municipal Securities Topic Page**

► **Fixed Income Topic Page**
Communications and Sales

Reg BI and Form CRS

Regulatory Obligations and Related Considerations

Regulatory Obligations

Reg BI establishes a “best interest” standard of conduct for broker-dealers and associated persons when they make a recommendation to retail customers of any securities transaction or investment strategy involving securities, including recommendations of types of accounts.

Broker-dealers are also required to provide a brief relationship summary, Form CRS, to retail investors on the types of client and customer relationship and services the firm offers; the fees, costs, conflicts of interest, and required standard of conduct associated with those relationships and services; whether the firm and its financial professionals currently have reportable legal or disciplinary history; and how to obtain additional information about the firm.

Related Considerations

- Does your firm have policies, procedures and controls in place to assess recommendations using a best interest standard?
- Do your firm and your associated persons apply a best interest standard to recommendations of types of accounts and recommendations to roll over or transfer assets from one type of account to another?
- Do your firm’s policies, procedures and controls continue to address compliance with FINRA Rule 2111 (Suitability), which still applies to recommendations made to non-retail investors?
- Does your firm have policies, procedures and controls addressing Reg BI’s recordkeeping requirements?
- Has your firm provided adequate Reg BI training to its sales and supervisory staff?
- Do your firm and your associated persons consider the express new elements of care, skill and costs when making recommendations to retail customers?
- Do your firm and your registered representatives guard against excessive trading, irrespective of whether the broker-dealer or associated person “controls” the account?
- Does your firm have policies and procedures to provide the disclosures required by Reg BI?
- Does the firm place any material limitations on the securities or investment strategies involving securities that may be recommended to a retail customer, and if so, does the firm address and disclose such limitations?
- Does your firm have policies and procedures to identify and address conflicts of interest?
- If the firm is not dually registered as an investment adviser, commodity advisor or municipal advisor, does the firm or any of its associated persons who are not dually registered advisors or advisory representatives use “adviser” or “advisor” in their name or title?
- Does your firm have policies, procedures and controls in place regarding the filing, updating and delivery of Form CRS?
- Does your firm’s Form CRS accurately respond to the disciplinary history question with regard to the firm and its financial professionals?
- If your firm has a website, has it posted its Form CRS in a prominent location on that website?
- Does your firm’s Form CRS include required conversation starters, headers and prescribed language?
Exam Findings and Effective Practices

As FINRA is in the early stages of reviewing for compliance with these new obligations, this Report will not include exam findings or effective practices relating to Reg BI and Form CRS. FINRA notes that the SEC held a virtual Roundtable on Regulation Best Interest and Form CRS that discussed some early examination findings. We anticipate issuing a separate publication in the future after more exams have been conducted. FINRA reminds firms to review the materials noted in the Additional Resources section below.

Additional Resources

- Regulatory Notice 20-18 (FINRA Amends Its Suitability, Non-Cash Compensation and Capital Acquisition Broker (CAB) Rules in Response to Regulation Best Interest)
- Regulatory Notice 20-17 (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- FINRA Highlights Firm Practices from Regulation Best Interest Preparedness Reviews
- SEC’s Regulation Best Interest, Form CRS and Related Interpretations
- FINRA’s Regulation Best Interest (Reg BI) Topic Page

Communications with the Public

Regulatory Obligations and Related Considerations

Regulatory Obligations

FINRA Rule 2210 (Communications with the Public) categorizes all communications into three categories—correspondence, retail communications or institutional communications—and sets principles-based content standards that are designed to apply to ongoing developments in communications technology and practices. The rule also includes standards for firms’ approval, review and recordkeeping procedures, as well as requirements to file certain communications with FINRA. FINRA Rule 2210 requires, among other things, that all communications be based on principles of fair dealing and good faith, be fair and balanced, provide a sound basis for evaluating the facts “in regard to any particular security or type of security, industry, or service” and include all “material fact[s] or qualification[s]” necessary to ensure such communications are not misleading. In addition, the rule prohibits false, misleading, promissory or exaggerated statements or claims, and projections of performance.

Related Considerations

- General Standards
  - Do your firm’s communications include material information necessary to make them fair, balanced and not misleading? For example, if a communication promotes the benefits of a high-risk or illiquid security, does it explain the associated risks?
  - Do your firm’s communications balance specific claims of investment benefits from a securities product or service (especially complex products) with the key risks specific to that product or service?
  - Do your firm’s communications contain false, misleading or promissory statements or claims?
  - Do your firm’s communications contain predictions or projections of investment performance to investors that are generally prohibited by FINRA Rule 2210(d)(1)(F)?
**Digital Communication Channels**

- Does your firm’s digital communication policy address all permitted and prohibited digital communication channels and features available to your customers and associated persons?
- Does your firm review for red flags that may indicate a registered representative is communicating through unapproved communication channels, and does your firm follow up on such red flags? For example, red flags might include email chains that copy unapproved representative email addresses, references in emails to communications that occurred outside approved firm channels, or customer complaints mentioning such communications.
- How does your firm supervise and maintain books and records in accordance with SEC and FINRA rules for all approved digital communications?
- If your firm offers an app to customers that includes an interactive element, does the information provided to customers constitute a “recommendation” that would be covered by Reg BI, which requires a broker-dealer to act in a retail customer’s “best interest,” or suitability obligations under FINRA Rule 2360 (Options)? If so, how does your firm comply with these obligations?
- If your firm’s app platform design includes “game-like” aspects that are intended to influence customers to engage in certain trading or other activities, how does your firm address and disclose the associated potential risks to your customers?
- Do your firm’s communications—regardless of the platform through which they are made—comply with the content standards set forth in FINRA Rule 2210?

**Digital Asset Communications** – If your firm or an affiliate engages in digital asset activities:

- Does your firm provide a fair and balanced presentation in marketing materials and retail communications, including addressing risks presented by digital asset investments, and not misrepresenting the extent to which digital assets are regulated by FINRA or the federal securities laws or eligible for protections thereunder, such as Securities Investor Protection Corporation (SIPC) coverage?
- Do your firm’s communications misleadingly imply that digital asset services offered through an affiliated entity are offered through and under the supervision, clearance and custody of a registered broker-dealer?

**Cash Management Accounts Communications** – If your firm offers Cash Management Accounts, does it:

- Clearly communicate the terms of the Cash Management Accounts?
- Disclose that the Cash Management Accounts’ deposits are obligations of the destination bank, and not cash balances held by your firm?
- Confirm that its communications do not state or imply that:
  - brokerage accounts are similar to, or the same, as bank “checking and savings accounts” or other accounts insured by the Federal Deposit Insurance Corporation (FDIC); and
  - FDIC insurance coverage applies to funds when held at or by a registered broker-dealer?
- Review whether communications fairly explain the:
  - nature and structure of the program;
  - relationship of the brokerage accounts to any partner banks in the Cash Management Accounts;
  - amount of time it may take for customer funds to reach the bank accounts; and
  - risks of participating in such programs?
Exam Findings and Effective Practices

Exam Findings

► Deficient Digital Assets Communications — Failing to balance promotional statements with prominent risk disclosures; including false, misleading or unwarranted statements; using the same firm names, websites and other materials for broker-dealers and their digital asset affiliates; not identifying the (non-broker-dealer) entities responsible for digital asset offerings; and implying that digital assets were offered by the broker-dealer.

► Misrepresentations in Cash Management Accounts Communications — Misrepresenting material information relating to Cash Management Accounts in online and other communications (in some cases, despite written and verbal warnings from FINRA’s Advertising Regulation Department), including, for example, the firms’ status as broker-dealers rather than banks; the status of Cash Management Accounts as “checking and savings accounts;” the amount of FDIC insurance coverage for the deposits; the amount of time it may take for customer funds to reach the bank accounts; terms of the Cash Management Accounts; and risks of participating in such programs.

► Insufficient Supervision and Recordkeeping for Digital Communication — Not maintaining policies and procedures to reasonably identify and respond to red flags—such as customer complaints, representatives' email, OBA reviews or advertising reviews—that registered representatives used impermissible business-related digital communications methods, including texting, messaging, social media, collaboration apps or “electronic sales seminars” in chatrooms.

► No WSPs and Controls for Communication That Use Non-Member or OBA Names (so-called “Doing Business As” or “DBA” Names) — Not maintaining WSPs to identify the broker-dealer clearly and prominently as the entity through which securities were offered in firm communications, such as websites, social media posts, seminars or emails that promote or discuss the broker-dealer’s securities business and identify a non-member entity, such as a representative's OBA; and not including a “readily apparent reference” and hyperlink to FINRA’s BrokerCheck in such communications.
Emerging Digital Communication Risks

New Digital Platforms With Interactive and “Game-Like” Features

2020 witnessed a surge in new retail investors entering the markets via online brokers, as well as an increase in certain types of trading, including options. Some online broker-dealers’ apps—as well as those offered by other financial services and consumer-oriented businesses—include interactive and “game-like” features, as well as related forms of advertising and marketing. Such features affect many aspects of how firms interact and communicate with customers, from initial advertisements through the opening of accounts, recommendations and the presentation of different investment choices.

While such features may improve customers’ access to firm systems and investment products, they may also result in increased risks to customers if not designed with the appropriate compliance considerations in mind. Firms must evaluate these features to determine whether they meet regulatory obligations to:

- comply with any Reg BI and Form CRS requirements if any communications constitute a “recommendation” that requires a broker-dealer to act in a retail customer’s “best interest”;
- make disclosures relating to risks to customers, fees, costs, conflicts of interest, and required standards of conduct associated with the firm’s relationships and services;
- prohibit the use of false, exaggerated or misleading statements or claims in any communications and ensure all firm communications are fair and balanced and do not omit material information concerning products or services;
- comply with account opening requirements that require firms to gather information about customers (such as FINRA Rule 4512 (Customer Account Information)) and approve certain types of accounts, including options accounts (such as FINRA Rule 2360(b)(16) (Diligence in Opening Accounts) and other supervisory controls relating to options, such as surveilling for options-related customer complaints, excessive commissions and fees, and large amounts of losses);
- develop a comprehensive supervisory system for such communication methods, including surveilling for red flags of potential violative behavior and maintaining books and records of all communications related to the firm’s business as such; and
- address compliance with FINRA communications rules, such as FINRA Rules 2210 (Communications with the Public); 2211 (Communications with the Public About Variable Life Insurance and Variable Annuities); 2212 (Use of Investment Company Rankings in Retail Communications); 2213 (Requirements for the Use of Bond Mutual Fund Volatility Ratings); 2214 (Requirements for Use of Investment Analysis Tools); 2215 (Communications with the Public Regarding Securities Futures); 2216 (Communications with the Public Regarding Collateralized Mortgage Obligations) and 2220 (Options Communications).
Effective Practices

► **Comprehensive Procedures for Digital Communications** – Maintaining and implementing procedures for firm digital communication channel policies, including:
  - **Monitoring of New Tools and Features** – Marketing, compliance and information technology departments working closely together, as well as with third-party vendors, to monitor new communication channels, apps and features available to their associated persons and customers.
  - **Defining and Enforcing What is Permissible and Prohibited** – Clearly defining permissible and prohibited digital communication channels, and blocking prohibited channels, tools or features, including those that prevent firms from complying with their recordkeeping requirements.
  - **Supervision** – Implementing supervisory review procedures tailored to each digital channel, tool and feature.
  - **Video Content Protocols** – Developing WSPs and controls for live-streamed public appearances, scripted presentations or video blogs.
  - **Training** – Implementing mandatory training programs prior to providing access to firm-approved digital channels, including expectations for business and personal digital communications and guidance for using all permitted features of each channel.
  - **Disciplinary Action** – Temporarily suspending or permanently blocking from certain digital channels or features those registered representatives who did not comply with the policies and requiring additional digital communications training.

► **Digital Asset Communications** – Maintaining and implementing procedures for firm digital asset communications, including:
  - **Risk Disclosure** – Prominently describing the risks associated with digital assets, including that such investments are speculative, involve a high degree of risk, are generally illiquid, may have no value, have limited regulatory certainty, are subject to potential market manipulation risks and may expose investors to loss of principal.
  - **Communication Review** – Reviewing firms’ communications to confirm that they were not exaggerating the potential benefits of digital assets or overstating the current or future status of digital asset projects or platforms.
  - **Communication to Differentiate Digital Assets From Broker-Dealer Products** – Identifying, segregating and differentiating firms’ broker-dealer products and services from those offered by affiliates or third parties, including digital asset affiliates; and clearly and prominently identifying entities responsible for non-securities digital assets businesses (and explaining that such services were not offered by the broker-dealer or subject to the same regulatory protections as those available for securities).

► **Reviews of Firms’ Capabilities for Cash Management Accounts** – Requiring new product groups or departments to conduct an additional review for proposed Cash Management Accounts to confirm that the firms’ existing business processes, supervisory systems and compliance programs—especially those relating to communications—can support such programs.

► **Use of Non-Member or OBA Names (so-called DBAs)** – Maintaining and implementing procedures for OBA names, including:
  - **Training** – Providing training on relevant FINRA rules and firm policies, and requiring annual attestations to demonstrate compliance with such requirements.
  - **Templates** – Requiring use of firm-approved vendors to create content or standardized templates populated with approved content and disclosures for all OBA communications (including websites, social media, digital content or other communications) that also concern the broker-dealer’s securities business.
Prior Approval – Prohibiting the use of OBA communications that concern the broker-dealer’s securities business without prior approval by compliance, and creating a centralized system for the review and approval of such communications, including content and disclosures.

Notification and Monitoring – Requiring registered representatives to notify compliance of any changes to approved communications, and conducting periodic, at least annual, monitoring and review of previously approved communications for changes and updates.

Additional Resources
- Regulatory Notice 20-23 (FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- Regulatory Notice 20-21 (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- Regulatory Notice 19-31 (Disclosure Innovations in Advertising and Other Communications with the Public)
- Regulatory Notice 17-18 (Guidance on Social Networking Websites and Business Communications)
- Regulatory Notice 11-39 (Social Media Websites and the Use of Personal Devices for Business Communications)
- Regulatory Notice 10-06 (Guidance on Blogs and Social Networking Web Sites)
- Advertising Regulation Topic Page
- Social Media Topic Page

Private Placements

Regulatory Obligations and Related Considerations

Regulatory Obligations
As noted in Regulatory Notice 10-22 (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings), as part of their obligations under FINRA Rule 2111 (Suitability) and supervisory requirements under FINRA Rule 3110 (Supervision), firms must conduct a “reasonable investigation” by evaluating “the issuer and its management; the business prospects of the issuer; the assets held by or to be acquired by the issuer; the claims being made; and the intended use of proceeds of the offering.” The SEC’s Reg BI became effective on June 30, 2020, and would apply to recommendations of private offerings to retail customers. Reg BI similarly requires, among other things, a broker-dealer to exercise reasonable diligence, care and skill to understand the potential risks, rewards and costs associated with a private offering recommendation and have a reasonable basis to believe that the private offering recommendation could be in the best interest of at least some retail customers.

In addition, firms must make timely filings for specified private placement offerings with FINRA’s Corporate Financing Department under FINRA Rules 5122 (Private Placements of Securities Issued by Members) and 5123 (Private Placements of Securities).

Related Considerations
- What policies and procedures does your firm have to address filing requirements and timelines under FINRA Rules 5122 and 5123? How does it review for compliance with such policies?
- How does your firm use and evaluate consultants, experts or other third-party vendors’ due diligence reports?
How does your firm conduct reasonable investigations on private placement offerings, including conducting further inquiry into red flags identified during the reasonable investigation process?

How does your firm address conflicts of interest identified in third-party due diligence reports?

How does your firm handle escrowed funds and amended terms in contingency offerings?

If your firm is engaging in new business, such as Regulation A offerings or SPACs, has it implemented WSPs to address this business? If this business may constitute a material change in your firm’s business operations, has your firm considered whether it needs to file a Continuing Membership Application (CMA)?

Exam Findings and Effective Practices

Exam Findings

- **Late Filings** — Not having policies and procedures, processes and supervisory programs to comply with filing requirements; and failing to make timely filings (with, in some cases, delays lasting as long as six to twelve months after the offering closing date).

- **No Reasonable Investigation** — Failing to perform reasonable investigations of private placement offerings prior to recommending the offerings to retail investors, including failing to conduct additional research about new offerings, relying on their experience with the same issuer in previous offerings and not conducting further inquiry into red flags identified during the investigation process.

- **Concerning Third-Party Due Diligence** — Failing to address red flags (such as disciplinary history of the issuer’s management), conflicts of interest (such as undisclosed direct or indirect common ownership of affiliated entities or the issuer) or significant concerns (such as no legitimate operating history for the issuer) identified in third-party due diligence reports.

Effective Practices

- **Private Placement Checklist** — Creating checklists with—or added to existing firm Regulation D and other offering checklists—all steps, filing dates, related documentation requirements and evidence of supervisory principal approval for the filing requirements of FINRA Rules 5122 and 5123.

- **Independent Research** — Conducting and documenting independent research on material aspects of the offering; identifying any red flags with the offering or the issuer (such as questionable business plans or unlikely projections or results); and addressing and, if possible, resolving concerns that would be relevant to a potential investor (such as tax considerations or liquidity restrictions).

- **Independent Verification** — Verifying information that was key to the performance of the offering (such as unrealistic costs projected to execute the business plan coupled with aggressively projected timing and overall rate of return for investors); and, in some cases, receiving support from due diligence firms, experts and third-party vendors.

- **Mitigating Conflicts of Interest** — Using firms’ reasonable investigation processes to mitigate conflicts of interest and developing comprehensive disclosures for offerings involving firm affiliates or issuers whose control persons were also employed by the firm.

- **Ownership for Filings** — Assigning responsibility for private placement filing requirements to specific individual(s) or team(s) and conducting targeted, in-depth training about the firms’ policies, process and technical filing requirements.

- **Automated Alert System** — Creating an automated system that alerts responsible individual(s) and supervisory principal(s) about upcoming and missed filing deadlines.
Private Placement Committee – Creating a private placement committee (at larger firms) or formally designating one or more qualified persons (at smaller firms); charging committee-designated individuals with investigating and determining whether to approve the offering for sale to investors; and conducting research and identifying and highlighting red flags with the offering or the issuer.

Post-Approval Processes – Using the investigation analysis to establish post-approval processes and investment limits based on the complexity or risk level of the offering.

Ongoing Monitoring – Conducting ongoing monitoring after the offering to ascertain whether offering proceeds were used in a manner consistent with the offering memorandum, particularly for ongoing sales of an offering after initial closing.

Additional Resources

- Regulatory Notice 20-21 (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- Regulatory Notice 10-22 (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings)
- Report Center – Corporate Financing Report Cards
- FAQs about Private Placements
- Corporate Financing Private Placement Filing System User Guide
- Private Placements Topic Page

Variable Annuities

Regulatory Obligations and Related Considerations

Regulatory Obligations

FINRA Rule 2330 (Members’ Responsibilities Regarding Deferred Variable Annuities) establishes sales practice standards regarding recommended purchases and exchanges of deferred variable annuities, including requiring a reasonable belief that the customer has been informed of the various features of annuities (such as surrender charges, potential tax penalties, various fees and costs, and market risk); and, prior to recommending the purchase or exchange of a deferred variable annuity, requiring reasonable efforts to determine the customer’s age, annual income, investment experience, investment objectives, investment time horizon, existing assets and risk tolerance. To the extent that a broker-dealer or associated person is recommending a purchase or exchange of a deferred variable annuity to a retail customer, Reg BI’s obligations, discussed above, also would apply.

In addition, the rule requires that firms conduct surveillance to determine if any associated person is effecting deferred variable annuity exchanges at a rate that might suggest conduct inconsistent with FINRA Rule 2330. Firms must also have procedures to implement corrective action to address any exchanges and conduct that violate FINRA Rule 2330.

Related Considerations

- How does your firm review for rates of variable annuity exchanges (i.e., does your firm use any automated tools, exception reports or surveillance reports)?
- Does your firm have standardized review thresholds for rates of variable annuity exchanges?
> Does your firm have a process to confirm its variable annuity data integrity (including general product information, share class, riders and exchange-based activity) and engage with affiliate and non-affiliate insurance carriers to address inconsistencies in available data, data formats and reporting processes for variable annuities?

> What is your firm’s process to supervise buyout offers (i.e., does it include pre-approval, exception reports and post-transaction reviews)?

> What do your WSPs require registered representatives to do in order to support a determination that a transaction meets the standard of care requirements and that there is a reasonable basis for it? What is the manner in which they are to obtain, evaluate and record such information such as whether a customer would incur a surrender charge; would be subject to a new surrender period; would lose existing benefits; would be subject to increased fees or charges; would invest a substantial portion of the customer’s liquid net worth in the variable annuity; has liquidity needs that are inconsistent with the variable annuity; would be investing in a share class that is not in the customer’s best interest given his or her financial needs, time horizon and riders included with the contract; and has had another exchange within the preceding 36 months?

> Do your firm’s policies and procedures require registered representatives to inform customers of the various features of annuities, such as surrender charges, potential tax penalties, various fees and costs, and market risk?

> How do your firm’s registered principals supervise variable annuity transactions, including verifying how the customer would benefit from certain features of deferred variable annuities, such as tax-deferral, annuitization, or a death or living benefit? What processes, forms, documents and information do the firm’s registered principals rely on to make such determinations?

> Does your firm have WSPs to address when it decides to stop selling or retires certain products, or opens buyout or exchange periods, including, but not limited to: how it will handle the product termination process; how it decides whether it offers an exchange or buyout; the scope of its exposure (in terms of contracts and customers); how it will notify customers and registered representatives; and how it will monitor for exchange rates?

### Exam Findings and Effective Practices

#### Exam Findings

> **Not Addressing Buyouts** – Not addressing within firms’ systems of supervision (by having applicable WSPs, delivering training, or making appropriate disclosures, etc.) that customers accepting buyouts may be losing valuable benefits associated with their existing products, subject to new surrender charge periods, and paying higher fees and expenses with new products (as was the case when customers were impacted by a recent announcement that an insurer with sizable variable annuity assets will terminate servicing agreements, cancel certain trail commissions for registered representatives, and provide buyout offers to its variable annuity customers).

> **Unsuitable Exchanges** – Not reasonably supervising recommendations of exchanges that were inconsistent with the customer’s objectives and time horizon and resulted in, among other consequences, increased fees to the customer or the loss of material, paid-for accrued benefits.

> **Inadequate Source of Funds Review** – Not performing sufficient review of source of funds used to purchase new variable annuities.

> **Insufficient Training** – Not conducting training for registered representatives and supervisors regarding how to assess fees, surrender charges and long-term income riders to determine whether exchanges were suitable for customers.
Effective Practices

Buyout Offers

- **Policies and Reviews** – Performing a holistic review of buyout offers; requiring supervisory principal pre-approval (and, in some cases, additional second-level approval) for buyout offers; and requiring registered representatives’ recommendations to consider all changes to customers’ variable annuities, such as possible surrender charges, loss of benefits, contract values, riders, cash surrender values, expenses and fees.

- **Training** – Providing extensive, ongoing training and communications to all registered representatives about buyout offers and related compliance obligations (including, in some cases, creating dedicated firm telephone or chat helplines).

- **Conflicts of Interest** – Addressing and mitigating potential conflicts of interest for registered representatives who may recommend that customers pursue buyout offers to free up proceeds for new investments or variable annuity exchanges by, for example, leveling registered representatives’ compensation for buyout offers, exchanges or new investments.

- **Additional Disclosures** – Developing new buyout offer disclosures or expanding existing variable annuity disclosure forms to address considerations for buyout offers.

- **Additional Post-Transaction Review** – Creating additional exception reports and conducting additional transaction monitoring for those customers who accepted buyout offers to confirm that those transactions were submitted for supervisory principal pre-approval (and, where required, additional second-level approval) and, if not, evaluating for compliance with FINRA Rule 2330.

Exchanges

- **Automated Surveillance** – Using automated tools, exception reports and surveillance to review variable annuity exchanges, and implementing second-level supervision of supervisory reviews of exchange-related exception reports and account applications.

- **Rationales** – Requiring registered representatives to provide detailed written rationales for variable annuity exchanges for each customer (including confirming that such rationales address the specific circumstances for each customer and do not replicate rationales provided for other customers); and requiring supervisory principals to verify the information provided by registered representatives, including product fees, costs, rider benefits and existing product values.

- **Review Thresholds** – Standardizing review thresholds for rates of variable annuity exchanges; and monitoring for emerging trends across registered representatives, customers, products and branches.

- **Data Integrity** – Creating automated (rather than manual) solutions to synthesize variable annuity data (including general product information, share class, riders and exchange-based activity) and engaging with affiliated and non-affiliated insurance carriers to address inconsistencies in available data, data formats and reporting processes for variable annuities.

Additional Resources


- **Regulatory Notice 20-17** (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)

- **Regulatory Notice 10-05** (FINRA Reminds Firms of Their Responsibilities Under FINRA Rule 2330 for Recommended Purchases or Exchanges of Deferred Variable Annuities)
COMMUNICATIONS AND SALES | VARIABLE ANNUITIES

- *Notice to Members 07-06* (Special Considerations When Supervising Recommendations of Newly Associated Registered Representatives to Replace Mutual Funds and Variable Products)
- *Notice to Members 99-35* (The NASD Reminds Members of Their Responsibilities Regarding the Sales of Variable Annuities)
- Variable Annuities Topic Page
- SEC’s Regulation Best Interest, Form CRS and Related Interpretations
- FINRA’s Regulation Best Interest (Reg BI) Topic Page
Market Integrity

CAT

Regulatory Obligations and Related Considerations

Regulatory Obligations
FINRA and the national securities exchanges have adopted rules requiring their members to comply with Exchange Act Rule 613 and the CAT NMS Plan FINRA Rule 6800 Series (Consolidated Audit Trail Compliance Rule) (collectively, CAT Rules), which cover reporting to the CAT; clock synchronization; time stamps; connectivity and data transmission; development and testing; recordkeeping; the timeliness, accuracy and completeness of data; and compliance dates. Regulatory Notice 20-31 (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT) describes certain practices and recommended steps firms should consider when developing and implementing their CAT Rules compliance program.

Related Considerations

- Do your firm’s CAT Rules WSPs, at a minimum: (1) identify the individual, by name or title, responsible for the review of CAT reporting; (2) describe specifically what type of review(s) will be conducted of the data posted on the CAT Reporter Portal; (3) specify how often the review(s) will be conducted; and (4) describe how the review(s) will be evidenced?
- How does your firm confirm that the data reported by your firm or on your firm’s behalf is transmitted in a timely fashion and is complete and accurate?
- How does your firm determine how and when clocks are synchronized, who is responsible for clock synchronization, how your firm evidences that clocks have been synchronized, and how the firm will self-report clock synchronization violations?
- Does your firm conduct daily reviews of the Industry Member CAT Reporter Portal (CAT Reporter Portal) to, among other requirements, review file status to ensure the file(s) sent by the member or by their reporting agent was accepted by CAT and to identify/address any file submission or integrity errors?
- Does your firm conduct periodic comparative reviews of accepted CAT data against order and trade records and the CAT Reporting Technical Specifications?
- Does your firm communicate regularly with your CAT reporting agent, review relevant CAT guidance and announcements, and report CAT reporting issues to the FINRA CAT Help Desk?

Exam Findings and Effective Practices
As FINRA is in the early stages of reviewing for compliance with certain CAT Rules obligations, this Report does not include exam findings or effective practices relating to CAT Rules. FINRA reminds firms to review the materials noted in the Additional Resources section below.

Additional Resources

- Regulatory Notice 19-19 (FINRA Reminds Firms to Register for CAT Reporting by June 27, 2019)
- Regulatory Notice 17-09 (The National Securities Exchanges and FINRA Issue Joint Guidance on Clock Synchronization and Certification Requirements Under the CAT NMS Plan)
- CAT NMS Plan
- Consolidated Audit Trail (CAT) Topic Page
Best Execution

Regulatory Obligations and Related Considerations

Regulatory Obligations

FINRA Rule 5310 (Best Execution and Interpositioning) requires that, in any transaction for or with a customer or a customer of another broker-dealer, a member and persons associated with a member shall use reasonable diligence to ascertain the best market for the subject security, and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions. Firms must conduct a “regular and rigorous” review of the execution quality of customer orders if the firm does not conduct an order-by-order review. Where “regular and rigorous” reviews are used instead of order-by-order reviews, the reviews must be performed at a minimum on a quarterly basis and on a security-by-security, type-of-order basis (e.g., limit order, market order and market on open order). If a firm identifies material differences in execution quality among the markets that trade the securities under review, it should modify its routing arrangements or justify why it is not doing so.

Related Considerations

- How does your firm determine whether to employ order-by-order or “regular and rigorous” reviews of execution quality?
- How does your firm implement and conduct an adequate “regular and rigorous” review of the quality of the executions of its customers’ orders?
- How does your firm address potential conflicts of interest in order-routing decisions, including those relating to its routing of orders to affiliated alternative trading systems (ATSSs), affiliated broker-dealers, or affiliated exchange members? When routing orders to an affiliate, how does your firm ensure that its order-routing decisions are based upon best execution considerations and not unduly influenced by these affiliations?
- How does your firm address potential conflicts of interest in order-routing decisions, including those related to its routing of orders to market centers that provide payment for order flow (PFOF) or other-routing inducements?
- When routing to market centers that provide PFOF or other inducements, how does your firm ensure that its order-routing decisions are based upon best execution considerations and not unduly influenced by these economic incentives?
- If your firm engages in fixed income and options trading, has it established targeted controls to perform its best execution obligations for these products? Does your firm consider differences among security types within these products, such as the different characteristics and liquidity of U.S. Treasury securities compared to other fixed income securities?
- Does your firm perform its best execution obligations with respect to trading conducted in both regular and extended trading hours?
- Does your firm consider the risk of information leakage when assessing the execution quality of orders routed to a particular venue?
- What data sources does your firm use for its routing decisions and execution quality reviews for different order types and sizes, including odd lots?
- How does your firm handle fractional share investing in the context of its best execution obligations?
Exam Findings and Effective Practices

Exam Findings

- **No Assessment of Execution vs. Competing Markets** – Not comparing the quality of the execution obtained via firms’ existing order-routing and execution arrangements against the quality of execution they could have obtained from competing markets.

- **No Review of Certain Order Types** – Not conducting adequate reviews on a type-of-order basis, including, for example, on market, marketable limit or non-marketable limit orders.

- **No Evaluation of Required Factors** – Not considering certain factors set forth in FINRA Rule 5310 when conducting a “regular and rigorous review,” including, among other things, speed of execution, price improvement and the likelihood of execution of limit orders; and using routing logic that was not necessarily based on quality of execution.

- **Conflicts of Interest** – Not considering and addressing potential conflicts of interest relating to routing of orders to affiliated broker-dealers, ATSSs or market centers that provide PFOF or other routing inducements, such as PFOF from wholesale market makers and exchange liquidity rebates.

- **Inadequate SEC Rule 606 Disclosures** – Not providing material disclosures in order-routing reports, such as the specific, material aspects of the non-directed order flow routed to firms’ trading desks, including that they stand to share in 100 percent of the profits generated by their trading as principal with their customers’ orders; material aspects of their relationships with each of the significant venues identified on their reports, including descriptions and terms of all arrangements for PFOF (including the amounts of PFOF on a per share or per order basis) and profit-sharing relationships that may have influenced the firms’ order routing decisions.

### Targeted Examination Letter on Zero Commissions

As part of FINRA’s ongoing 2020 targeted review of firms’ decisions to move to “zero-commission” trading, we are evaluating:

- whether the “zero-commission” model adversely affected firms’ compliance with their best execution obligations;

- how firms used other practices, such as Cash Management Accounts and PFOF, to potentially offset lost commission revenue; and

- whether firms prominently communicated restrictions and limitations of “zero-commission” structures and other fees charged to customers.

We will share the findings from this targeted review with member firms in a future publication once the review is complete.
Effective Practices

- **Exception Reports** – Using exception reports and surveillance reports to support firms’ efforts to meet their best execution obligations.
- **PFOF Order Routing Impact Review** – Reviewing how PFOF affects the order-routing process, including the following factors: any explicit or implicit contractual arrangement to send order flow to a third-party broker-dealer; terms of these agreements; whether it is on a per share basis or per order basis; and whether it is based upon the type of order, size of order, type of customer or the market class of the security.
- **Risk-Based “Regular and Rigorous Reviews”** – Conducting “regular and rigorous” reviews, at a minimum, on a quarterly basis, but depending on the firm’s business model, conducting reviews more frequently than quarterly (such as monthly).
- **Continuous Updates** – Updating WSPs and best execution analysis to address account, market and technology changes.

Additional Resources

- **Regulatory Notice 15-46** (Guidance on Best Execution Obligations in Equity, Options and Fixed Income Markets)
- **Notice to Members 01-22** (NASD Regulation Reiterates Member Firm Best Execution Obligations And Provides Guidance to Members Concerning Compliance)
- **Report Center, Equity Report Cards** – FINRA’s Best Execution Outside-of-the-Inside Report Card

Large Trader Reporting

Regulatory Obligations and Related Considerations

**Regulatory Obligations**

Exchange Act Rule 13h-1 (Large Trader Rule) requires “large traders” to identify themselves as such to the SEC, disclose to other firms their large trader status and, in certain situations, comply with certain filing, recordkeeping and reporting requirements. These requirements help the SEC identify large traders and obtain trading information about their activity in the U.S. securities markets. In addition, broker-dealers will be required to obtain and report large trader information to the CAT for accounts with CAT Reportable Events.

**Related Considerations**

- Has your firm created new WSPs or updated your WSPs to address the Large Trader Rule?
- Does the firm report its relevant proprietary trading activity with the designated Large Trader ID (LTID)?
- If not, how does your firm conduct daily calculations of its own trading activity to monitor its Large Trader status?
- Has your firm updated your new customer account process to address Large Trader Rule requirements?
- Does your firm perform daily calculations of customer accounts to determine if there were any new accounts that breached the daily or monthly thresholds?
- How does your firm notify customers of their regulatory obligations if the customer has been deemed to be an “Unidentified Large Trader”?
- How does your firm work with your clearing firm to comply with the Large Trader Rule?
- How is your firm preparing to comply with CAT reporting requirements relating to LTIDs?
Exam Findings and Effective Practices

Exam Findings

- **No WSPs** – Failing to update or create new WSPs to address the Large Trader Rule, including requirements for timely filing of Form 13H and identifying, monitoring, recordkeeping and filing for large traders and Unidentified Large Traders.
- **No Monitoring for Unidentified Large Traders** – Not monitoring customer activity to identify and detect Unidentified Large Traders and notifying such traders of their obligations.
- **Failure to Report LTID** – Not reporting the LTID on Electronic Blue Sheet (EBS) submissions for applicable orders.

Effective Practices

- **WSPs** – Creating new or updated WSPs to address the Large Trader Rule, including developing WSPs to comply with the Large Trader Rule’s recordkeeping requirements for its customer and proprietary trading businesses and Form 13H filing requirements for its proprietary business.
- **Form 13H Review** – Reviewing the accuracy of, and confirming any updates for, the firms’ Form 13H.
- **Large Trader Check** – Adding a large trader check to firms’ EBS policies and procedures to confirm that the LTID was populated and formatted correctly.
- **New Customer Account Process** – Requiring new institutional accounts to provide their LTID as part of the account opening process and, unless customers directed otherwise, requiring their LTIDs be applied to all of their new accounts.
- **Daily Large Trader and Customer Account Monitoring** – Completing daily large trader monitoring calculations to monitor the firms’ large trader status; performing daily large trader monitoring calculations for their customer accounts to determine if there were any new accounts that breached the daily or monthly thresholds; and engaging their clearing firm to confirm that the clearing firm provided accurate customer LTID numbers and these numbers remained up to date.
- **Unidentified Large Traders** – Unless customers justified their exemption from the Large Trader Rule:
  - creating Unidentified Large Trader ID for those customers;
  - notifying them of potential registration obligations; and
  - advising them to request their LTID.

Additional Resources

- Regulatory Notice 18-04 (FINRA and ISG Announce Extension of Effective Date for Certain Electronic Blue Sheet Data Elements and Updates to Certain Requestor and Exchange Codes)
- FINRA’s *Frequently Asked Questions about Electronic Blue Sheets (EBS)*
Market Access

Regulatory Obligations and Related Considerations

Regulatory Obligations
Exchange Act Rule 15c3-5 (Market Access Rule) requires broker-dealers with market access or that provide market access to their customers to “appropriately control the risks associated with market access so as not to jeopardize their own financial condition, that of other market participants, the integrity of trading on the securities markets, and the stability of the financial system.”

Related Considerations
► If your firm has market access, or provides it, does it have reasonably designed risk-management controls and WSPs to manage the financial, regulatory or other risks associated with this business activity?
► If your firm is highly automated, how does it manage and deploy technology changes for systems associated with market access, and what controls does it use, such as kill switches, to monitor and respond to aberrant behavior by trading algorithms or other impactful marketwide events?
► How does your firm adjust credit limit thresholds for customers, including institutional customers (whether temporary or permanent)?
► Does your firm use any automated controls to timely revert *ad hoc* credit limit adjustments?
► If your firm uses third-party vendor tools to comply with its Market Access Rule obligations, does it review during vendor due diligence whether the vendor can meet the obligations of the rule, and how does your firm maintain direct and exclusive control of applicable thresholds?
► What type of training does your firm provide to individual traders regarding the steps and requirements for requesting *ad hoc* credit limit adjustments?
► Does your firm test your firm’s market access controls, including fixed income controls, and how do you use that test for your firm’s annual CEO certification attesting to your firm’s controls?

Exam Findings and Effective Practices

Exam Findings
► Insufficient Controls – No pre-trade order limits, pre-set capital thresholds and duplicative and erroneous order controls for accessing ATSs, especially for fixed income transactions; unsubstantiated capital and credit pre-trade financial controls; no policies and procedures to govern intra-day changes to firms’ credit and capital thresholds, including requiring or obtaining approval prior to adjusting credit or capital thresholds, documenting justifications for any adjustments, and ensuring thresholds for temporary adjustments revert back to their pre-adjusted values.
► Inadequate Financial Risk Management Controls – For firms with market access, or those that provide it, inappropriate capital thresholds for trading desks, aggregate daily limits, or credit limits for institutional customers and counterparties.
► Reliance on Vendors – Relying on third-party vendors’ tools, including those of an ATS, to effect their financial controls, without understanding how vendors’ controls worked, and not maintaining direct and exclusive control over controls; and allowing the ATS to set capital thresholds for firms’ fixed income orders instead of establishing their own thresholds (some firms were not sure what their thresholds were, and had no means to monitor their usage during the trading day).
Effective Practices

- **Pre-Trade Fixed Income Financial Controls** – Implementing systemic pre-trade “hard” blocks to prevent fixed income orders from reaching an ATS that would cause the breach of a threshold.

- **Intra-day (Ad Hoc) Adjustments** – Implementing processes for requesting, approving, reviewing and documenting ad hoc credit threshold increases, and returning the limits to their original values as needed.

- **Tailored Erroneous or Duplicative Order Controls** – Tailoring firms’ erroneous or duplicative order controls to particular products, situations or order types, and preventing the routing of a market order based on impact (Average Daily Volume Control) that are set at reasonably high levels (particularly in thinly traded securities); and calibrating to reflect, among other things, the characteristics of the relevant securities, the business of the firm, and market conditions.

- **Post-Trade Controls and Surveillance** – When providing direct market access via multiple systems, including sponsored access arrangements, employing reasonable controls to confirm that those systems’ records were aggregated and integrated in a timely manner and conducting holistic post-trade and supervisory reviews for, among other things, potential manipulative trading patterns.

- **Testing of Financial Controls** – Periodically testing their market access controls, which forms the basis for an annual CEO certification attesting to firms’ controls.

Additional Resources

- **Regulatory Notice 16-21** (SEC Approves Rule to Require Registration of Associated Persons Involved in the Design, Development or Significant Modification of Algorithmic Trading Strategies)

- **Regulatory Notice 15-09** (Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies)

- Algorithmic Trading Topic Page

- Market Access Topic Page

Vendor Display Rule

Regulatory Obligations and Related Considerations

Regulatory Obligations

Rule 603 of Regulation NMS (Vendor Display Rule) generally requires broker-dealers to provide a consolidated display of market data for NMS stocks for which they provide quotation information to customers. Rule 600(b)(14) of Regulation NMS provides that the consolidated display includes “(i) the prices, sizes, and market identifications of the national best bid and national best offer for a security; and (ii) consolidated last sale information for a security,” while Rule 600(b)(15) of Regulation NMS provides that “consolidated last sale information” includes “the price, volume, and market identification of the most recent transaction report for a security that is disseminated pursuant to an effective national market system plan.”

Related Considerations

- Which firm systems or platforms provide quotation information to customers?

- How does your firm monitor whether the current quotation information is distributed to customers?

- Does your firm make the quotation information available to customers when they are placing their orders?

- Does your firm review the quotation information received from the Securities Information Processor (SIP) or vendors to determine whether that information is in compliance with all the requirements of SEC Rule 603?
Exam Findings and Effective Practices

Exam Findings

► Failure to Provide Consolidated Display
  - Missing Consolidated Display — Failing to provide the entire consolidated display:
    - in all contexts and relevant stages in which a customer may make a trading or routing decision, (such as at point of order entry and order modification); and
    - across all platforms where customers may make a trading or routing decision (such as displaying all elements of the consolidated display on firms’ web-based but not mobile device platforms).
  - Missing Elements — Providing the consolidated display, but not including certain elements, such as:
    - national best bid and offer (NBBO) (while providing only the last sale information);
    - last sale information (while providing only the NBBO);
    - market identification for NBBO or last sale;
    - size associated with NBBO or last sale; and
    - real-time NBBO and last sale information (e.g., 15-minute delayed data).

► Insufficient WSPs — Failing to maintain WSPs to address the Vendor Display Rule, periodic testing and validation that they were providing the consolidated display, and review for timely delivery of the consolidated display to customers (including evaluating and addressing any potential system latencies).

Effective Practices

► Confirming Market Data Feeds — Confirming that firms received all market data feeds (including all exchanges) necessary to provide consolidated quote and last sale information to customers (including all prices, sizes and market identification data).

► Customer Platform Reviews — Performing a comprehensive review to confirm that firms provided the consolidated display to customers across all platforms where customers may make a trading or order-routing decision (including mobile platforms).

► Latency Monitoring — Monitoring for any delays or latency of the consolidated display, especially for mobile platforms, and then taking corrective action to confirm that the Consolidated Display information was current.

► SIP Validation — Performing periodic validation of quotation and last sale information against SIP data by creating screenshots of firms’ quotation and last sale information for each customer platform and comparing it to SIP quotation and last sale information data.

► Testing and Validation — Testing and validating the consolidated display prior to and after upgrades or enhancements to customer platforms.

Additional Resources

► Regulatory Notice 15-52 (SEC Staff Provides Insight Into Firms’ Obligations When Providing Stock Quote Information to Customers)

► Regulation NMS Topic Page
Financial Management

Net Capital

Regulatory Obligations and Related Considerations

Regulatory Obligations

Exchange Act Rule 15c3-1 (Net Capital Rule) requires that firms must at all times have and maintain net capital at specific levels to protect customers and creditors from monetary losses that can occur when firms fail. Exchange Act Rule 17a-11 requires firms to notify FINRA in the event their net capital falls below the “minimum amount required” by the Net Capital Rule.

Related Considerations

- How does your firm review its net capital treatment of assets to confirm that they are correctly classified for net capital purposes?
- How does your firm confirm that it has correctly identified and aged all failed-to-deliver contracts, properly calculated the applicable net capital charges and correctly applied the deductions to its net capital calculation?
- For firms with expense sharing agreements, what kind of allocation methodology does your firm use and what kind of documentation does your firm maintain to substantiate its methodology for allocating specific broker-dealer costs to the firm or an affiliate?

Exam Findings and Effective Practices

Exam Findings

- Inaccurate Classification of Receivables, Liabilities and Revenue – Incorrectly classifying receivables, liabilities and revenues, which resulted in inaccurate reporting of firms’ financial positions and, in some instances, a capital deficiency; incorrectly classifying non-allowable assets, such as large investments in certificates of deposit (CDs) because firms did not have a process to assess the net capital treatment of CDs pursuant to Exchange Act Rule 15c3-1(c)(2)(vi)(E); and not reviewing account agreements for CDs to determine whether they contained stipulations restricting withdrawals prior to maturity, including restricting their withdrawal or giving the bank discretion to permit or prohibit their withdrawal.

- Failed to Deliver and Failed to Receive Contracts (Fails) – Not having a process to correctly identify, track and age intra-month and end of the month Fails for firms’ operating an Exchange Act Rule 15a-6 chaperoning business, including:
  - Inaccurate Net Capital Charge – Failing to compute and apply the correct applicable net capital charge for aged Fails;
  - No Information from Clearing Firm – Failing to request or confirm receipt of timely information relating to Fails from their clearing firms;
  - Gaps in Policies and Procedures – Failing to address monitoring, reporting and aging of Fails in firms’ policies and procedures;
  - Incorrect Balance Sheets and FOCUS Reports – Failing to record Fails on firms’ balance sheet, and, as a result, filing incorrect FOCUS reports; and
  - No Blotters – Failing to maintain blotters for Fails.
Incorrect Capital Charges for Underwriting Commitments – Not maintaining an adequate process to assess moment-to-moment and open contractual commitment capital charges on underwriting commitments, and not understanding their role as it pertained to the underwriting (i.e., best efforts or firm commitment).

Inaccurate Recording of Revenue and Expenses – Using cash accounting to record revenue and expenses as of the date the money changes hands, rather than accrual accounting (where firms would record revenue and expenses as of the date that revenue is earned or expenses are incurred); and making ledger entries as infrequently as once per month, as a result of which firms did not have adequate context to determine the proper accrual-based transaction date.

Insufficient Documentation Regarding Expense-Sharing Agreements – Not delineating a method of allocation for payment; not allocating (fixed or variable) expenses proportionate to the benefit to the broker-dealer; or not maintaining sufficient documentation to substantiate firms’ methodologies for allocating specific broker-dealer costs—such as technology fees, marketing charges, retirement account administrative fees and employees’ compensation—to broker-dealers or affiliates.

Effective Practices

Net Capital Assessment – Performing an assessment of their net capital treatment of assets, including CDs, to confirm that they were correctly classified for net capital purposes.

Agreement Review – Obtaining from, and verifying with, banks the withdrawal terms of any assets, with particular focus on CD products, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset’s classification and its net capital charge for the terms of all assets, including CDs, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset’s classification and its net capital charge.

Training and Guidance – Developing guidance and training for Financial and Operational Principal and other relevant staff on Net Capital Rule requirements for Fails, including how to report Fails on their balance sheets, track the age of Fails and, if necessary, calculate any net capital deficit resulting from aged Fails.

Aging Review – Performing reviews to confirm that they correctly aged Fail contract charges and correctly applied a net capital deduction, when applicable, to their net capital calculation.

Collaboration with Clearing Firms – Clarifying WSPs to address clearing firms’ responsibilities regarding net capital requirements, including for Fails, and introducing firms engaging their clearing firms to confirm that:

1. introducing firms were receiving a record of all Fails on a daily basis (or at least monthly);
2. clearing firms’ reports included all of the required information; and
3. introducing firms were correctly interpreting the clearing firms’ reports (especially distinctions between trade date and settlement date and those dates’ implications for aging calculations for Fails).

Additional Resources

Interpretations of Financial and Operational Rules

Regulatory Notice 15-33 (Guidance on Liquidity Risk Management Practices)

Regulatory Notice 10-57 (Funding and Liquidity Risk Management Practices)

Notice to Members 03-63 (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers)

Funding and Liquidity Topic Page
Liquidity Management

Regulatory Obligations and Related Considerations

Regulatory Obligations
Effective liquidity controls are critical elements in a broker-dealer’s risk management framework. Exchange Act Rule 17a-3(a)(23) requires firms that meet the thresholds specified under the rule to make and keep current records documenting the credit, market, and liquidity risk management controls established and maintained by the firm to assist it in analyzing and managing the risks associated with its business. FINRA routinely reviews firms’ practices in these areas, and in Regulatory Notice 15-33 (Guidance on Liquidity Risk Management Practices) shared observations on liquidity management practices.

Related Considerations
- What departments at your firm are responsible for liquidity management?
- How often does your firm review and adjust its liquidity management plan and the stress test frameworks?
- Do your firm’s liquidity management practices include steps to address specific stress conditions and identify firm staff responsible for addressing those conditions? Does your firm have a process for accessing liquidity during a stress event and determining how the funding would be used?
- Does your firm’s contingency funding plan take into consideration the quality of collateral, term mismatches and potential counterparty losses of your firm’s financing desks (in particular, in repo and stock loan transactions)?
- What kind of stress tests (e.g., market or idiosyncratic) does your firm conduct? Does your firm conduct stress tests in a manner and frequency that is appropriate for your firm’s business model, for example tests limited to a single time horizon, or over multiple time horizons? Does your firm incorporate the results of those stress tests into your firm’s business model?

Exam Observations and Effective Practices

Exam Observations
- **Not Extending the Stress Test Period** – Failing to expand stress tests from a single time horizon to multiple time horizons (such as 10 days to 30 days or longer).
- **Not Modifying Business Models** – Failing to incorporate the results of firms’ stress tests into their business model.
- **No Liquidity Contingency Plans** – Failing to develop contingency plans for operating in a stressed environment with specific steps to address certain stress conditions, including identifying the firm staff responsible for enacting the plan, the process for accessing liquidity during a stress event and setting standards to determine how liquidity funding would be used.

Effective Practices
- **Liquidity Risk Management Updates** – Updating liquidity risk management practices to take into account a firm’s current business activities, including:
  - establishing governance around liquidity management, determining who is responsible for monitoring the firm’s liquidity position, how often they monitor that position, and how frequently they meet as a group; and
creating a liquidity management plan that considers:
  - quality of funding sources;
  - potential mismatches in duration between liquidity sources and uses;
  - potential losses of counterparties;
  - how the firm obtains funding in a business-as-usual (BAU) condition, and stressed conditions;
  - assumptions based on idiosyncratic and market-wide conditions; and
  - early warning indicators, and escalation procedures, if risk limits are breached.

**Stress Tests** – Conducting stress tests in a manner and frequency that considered the firm’s business model, including:
  - assumptions specific to the firm’s business, and based on historical data;
  - the firm’s sources and uses of liquidity, and if sources could realistically fund its uses in a stressed environment;
  - the potential impact of off-balance sheet items on liquidity;
  - frequency of conducting stress tests, in accordance with the risk and complexity of the firm’s business; and
  - periodic review of stress test results by appropriate governance groups.

### Additional Resources

- **Regulatory Notice 10-57** (Funding and Liquidity Risk Management Practices)
- **Funding and Liquidity Topic Page**

### Credit Risk Management

#### Regulatory Obligations and Related Considerations

**Regulatory Obligations**

Under the financial responsibility rules, and related supervisory obligations, firms need to properly capture, measure, aggregate, manage and report credit risk, including risk exposures that may not be readily apparent. Such responsibility can be incurred under clearing arrangements, prime brokerage arrangements (especially fixed income prime brokerage), “give up” arrangements, sponsored access arrangements (discussed above in the Market Access section) or principal letters. Further, firms should maintain a robust internal control framework where they manage credit risk and they identify and address all relevant risks covering the extension of credit to their customers and counterparties. Weaknesses within the firm’s risk management and control processes could result in a firm incorrectly capturing its exposure to credit risk.

**Related Considerations**

- Does your firm maintain a robust internal control framework to capture, measure, aggregate, manage, supervise and report credit risk?
Does your firm review whether it is accurately capturing its credit risk exposure, maintain approval and documented processes for increases or other changes to assigned credit limits and monitor exposure to affiliated counterparties?

Does your firm have a process to confirm it is managing the quality of collateral and monitoring for exposures that would have an impact on capital?

Exam Observations and Effective Practices

Exam Observations

- **No Credit Risk Management Reviews** – Not evaluating firms’ risk management and control processes to confirm whether they were accurately capturing their exposure to credit risk.

- **No Credit Limit Assignments** – Not maintaining approval and documentation processes for assignment, increases or other changes to credit limits.

- **No Monitoring Exposure** – Not monitoring exposure to firms’ affiliated counterparties.

Effective Practices

- **Credit Risk Framework** – Developing comprehensive internal control frameworks to capture, measure, aggregate, manage and report credit risk, including:
  - establishing house margin requirements;
  - identifying and assessing credit exposures in real-time environments;
  - issuing margin calls and margin extensions (and resolving unmet margin calls);
  - establishing the frequency and manner of stress testing for collateral held for margin loans and secured financing transactions; and
  - having a governance process for approving new, material margin loans.

- **Credit Risk Limit Changes** – Maintaining approval and documentation processes for increases or other changes to assigned credit limits, including:
  - having processes for monitoring limits established at inception, and on an ongoing basis, for customers and counterparties;
  - reviewing how customers and counterparties adhere to these credit limits, and what happens if these credit limits are breached; and
  - maintaining a governance structure around credit limit approvals.

- **Counterparty Exposure** – Monitored exposure to their affiliated counterparties, considering their:
  - creditworthiness;
  - liquidity and net worth;
  - track record of past performance (e.g., traded products, regulatory history, past arbitration and litigation); and
  - internal risk controls.

Additional Resources

- [Funding and Liquidity Topic Page](#)
Segregation of Assets and Customer Protection

Regulatory Obligations and Related Considerations

Regulatory Obligations
Exchange Act Rule 15c3-3 (Customer Protection Rule) imposes certain requirements on firms that are designed to protect customer funds and securities. Firms are obligated to maintain custody of customer securities and safeguard customer cash by segregating these assets from the firm’s proprietary business activities, and promptly deliver to their owner upon request. Firms can satisfy this requirement by either keeping customer funds and securities in their physical possession, or in a good control location that allows the firm to direct their movement (e.g., a clearing corporation).

Related Considerations

What is your firm’s process to prevent, identify, research and escalate new or increased deficits which are in violation of the Customer Protection Rule?
What controls does your firm have in place to identify and monitor its possession or control deficits, including the creation, cause and resolution?
If your firm claims an exemption from the Customer Protection Rule and it is required to forward customer checks promptly to your firm’s clearing firm, how does your firm implement consistent processes for check forwarding and maintain accurate blotters to demonstrate that checks were forwarded in a timely manner?
How does your firm train staff on Customer Protection Rule requirements?
What are your firm’s processes to confirm that your firm correctly completes its reserve formula calculation and maintains the amounts that must be deposited into the special reserve bank account(s)?
If your firm is engaging in digital asset transactions, what controls and procedures has it established to support facilitation of such transactions, including initial issuance or secondary market trading of digital assets? Has the firm analyzed these controls and procedures to address potential concerns that they may be viewed as a custodian (i.e., holding or controlling customer property)?

Exam Findings and Effective Practices

Exam Findings

Inconsistent Check-Forwarding Processes – Not implementing consistent processes for check forwarding to comply with an exemption from the Customer Protection Rule.
Inaccurate Reserve Formula Calculations – Failing to correctly complete reserve formula calculations due to errors in coding because of limited training and staff turnover, challenges with spreadsheet controls, limited coordination between various internal departments and gaps in reconciliation calculations.
Omitted or Inaccurate Blotter Information – Maintaining blotters with insufficient information to demonstrate that checks were forwarded in a timely manner and inaccurate information about the status of checks.

Effective Practices

Legal and Compliance Engagement – Collaborating with legal and compliance departments to confirm that all agreements supporting control locations are finalized and executed before the accounts are established and coded as good control accounts on firms’ books and records.
Addressing Conflicts of Interest – Confirming which staff have system access to establish a new good control location and that they are independent from the business areas to avoid potential conflicts of interest; and conducting ongoing review to address emerging conflicts of interest.

Reviews and Exception Reports for Good Control Locations – Conducting periodic review of and implementing exception reports for existing control locations for potential miscoding, out-of-date paperwork or inactivity.

Check-Forwarding Procedures – Creating and implementing policies to address receipt of customer checks, checks written to the firm, and checks written to a third party.

Check Forwarding Blotter Review – Creating and reviewing firms’ check received and forwarded blotters to confirm that they are up to date, and including the information required to demonstrate compliance with the Customer Protection Rule exemption.

Additional Resources

Customer Protection – Reserves and Custody of Securities (SEA Rule 15c3-3)


Appendix—Using FINRA Reports in Your Firm’s Compliance Program

Firms have shared the following ways they have used prior FINRA publications, such as Exam Findings Reports and Priorities Letters (collectively, Reports), to enhance their compliance programs. We encourage firms to consider these practices, if relevant to their business model, and continue to provide feedback on how they use FINRA publications.

- **Assessment of Applicability** – Performed a comprehensive review of the findings, observations and effective practices, and identified those that are relevant to their businesses.

- **Risk Assessment** – Incorporated the topics highlighted in our Reports into their overall risk assessment process and paid special attention to those topics as they performed their compliance program review.

- **Gap Analysis** – Conducted a gap analysis to evaluate how their compliance programs and WSPs address the questions noted in Priorities Letters and the effective practices in Exam Findings Reports, and determined whether their compliance programs have any gaps that could lead to the types of findings noted in Exam Findings Reports.

- **Project Team** – Created interdisciplinary project teams and workstreams (with staff from operations, compliance, supervision, risk, business and legal departments, among other departments) to:
  - assign compliance stakeholders and project owners;
  - summarize current policies and control structures for each topic;
  - engage the legal department for additional guidance regarding regulatory obligations;
  - develop plans to address gaps; and
  - implement effective practices that were not already part of their compliance program.

- **Circulation to Compliance Groups** – Shared copies of the publications or summaries of relevant sections with their compliance departments.

- **Presentation to Business Leaders** – Presented to business leadership about their action plans to address questions, findings, observations and effective practices from our Reports.

- **Guidance** – Used Reports to prepare newsletters, internal knowledge-sharing sites or other notices for their staff.

- **Training** – Added questions, findings, observations and effective practices from Reports, as well as additional guidance from firms’ policies and procedures, to their Firm Element and other firm training.
March 14, 2022

On March 9, 2022, the SEC released its newest series of proposed cybersecurity rules, this time for all public companies. Consistent with the proposed rules issued last month for investment advisers and funds, which we discussed here, the SEC continues to prioritize cybersecurity disclosures to the marketplace, placing particular emphasis on timely and detailed disclosures of material cybersecurity incidents, as well as on periodic disclosures about cybersecurity risk management and governance.

These detailed and broadly applicable proposed rules (which have registered dissent from Commissioner Hester Pierce) significantly expand upon the SEC’s 2018 statement and interpretive guidance for public companies on cybersecurity disclosures by promulgating a substantial new cybersecurity regulatory framework that creates significant new disclosure obligations for these entities. The proposed rules represent another step in the SEC’s overarching strategy to create cybersecurity regulations for entities within the SEC’s jurisdiction.

Key Requirements Under the Proposed Rules

- **Current Disclosure of Material Cybersecurity Incidents on Form 8-K.** Most notably, the proposed rules would require a registrant to disclose certain information about a material cybersecurity incident in a new Form 8-K line item within four business days of determining that a cyber incident it has experienced is material, rather than upon the discovery of the incident. Proposed Item 106(a) of Regulation S-K defines “cybersecurity incident” to include any “unauthorized occurrence on or conduct through a registrant’s information systems that jeopardizes the confidentiality, integrity, or availability” of the registrant’s information or information systems. The SEC noted that this definition should be broadly construed to include accidental data exposures, deliberate action to gain access to systems or steal/alter data, or other system compromises or data breaches.

To address any concern that some registrants may delay assessing materiality to avoid a disclosure obligation, proposed Item 1.05 requires the determination of...
materiality to be made “as soon as reasonably practicable after discovery of the incident.” The proposed rules would require these disclosures to include to the extent the information is known at the time of the 8-K filing: (1) the date the incident was discovered; (2) whether the incident is ongoing; (3) a brief description of the nature and scope of the incident; (4) an indication of whether any data was compromised; and (5) the potential effect of the incident on operations.

The proposed rules incorporate the well-settled Supreme Court precedent on materiality. Recognizing the fact-specific nature of the materiality inquiry, the proposed rules provide several examples of cybersecurity incidents that could be subject to disclosure, including business email compromises, data theft by internal or external actors, or ransomware. Notably, while the proposed rules would not provide a safe harbor for a reporting delay in the context of an ongoing internal or external investigation (such as one by law enforcement), they would provide for certain limited safe harbors, including from liability under Exchange Act Section 10(b) and Rule 10b-5 thereunder and protection against loss of Form S-3 or Form SF-3 eligibility. Additionally, while foreign private issuers are not required to file current reports on Form 8-K, General Instruction B of Form 6-K would be amended to reference material cybersecurity incidents among the items that may trigger a current report on Form 6-K.

- **Periodic Updates to Disclosures of Cybersecurity Incidents.** Proposed Item 106(d)(1) to Regulation S-K would also require a registrant to disclose any material changes in the registrant’s Quarterly Report on Form 10-Q or Annual Report on Form 10-K from the disclosures made in the initially filed Item 1.05 8-K. This may include changes in scope, additional information on whether data was altered or stolen, and the steps taken to address the incident. Further, the proposed rules provide a non-exhaustive list of potential disclosures that should be addressed in a registrant’s 10-Q or 10-K filings following a cybersecurity incident, including any material or future impact on operations and financial condition, status of the remediation efforts, and any changes to the registrant’s cybersecurity policies and procedures because of the incident.

Proposed Item 106(d)(2) of Regulation S-K would also require periodic disclosure of immaterial cybersecurity incidents that become material in the aggregate. Such matters could potentially include coordinated smaller but continuous cyber-attacks such as extended phishing campaigns or account takeovers if the registrant determines that the incidents are material in the aggregate. Similar to an Item 1.05 8-K disclosure for a single material event, these periodic disclosures should briefly describe the nature and scope of the incidents, whether data was stolen or altered, the impact to operations, and remediation efforts.
• **Periodic Disclosure of Risk Management and Governance.** Proposed Item 106(b) and (c) of Regulation S-K would also increase the scope and detail of registrant disclosures on cybersecurity risk management, strategy, and governance.

  • **Risk Management.** If adopted as is, proposed Item 106(b) of Regulation S-K would require “consistent and informative disclosure regarding [registrant] cybersecurity risk management and strategy[,]” potentially including disclosure of policies and procedures to manage cybersecurity risk. More specifically, to the extent applicable, registrants would be required to disclose the existence of a risk assessment program, engagement of any third-party auditors or consultants associated with the program, policies and procedures associated with third-party risk, and among other items, steps taken to prevent, detect, and minimize the effects of cybersecurity incidents.

  • **Governance.** Under proposed Item 106(c) of Regulation S-K, registrants would also be required to disclose their cybersecurity governance policies, including a discussion of the board and management’s role in identifying, assessing, and managing cybersecurity risk, as well as their experience in dealing with such risks. More specifically, as it pertains to the board’s oversight, registrants would be required to identify: (1) which board committee or directors are responsible for overseeing cybersecurity risks; (2) how the board is informed of cybersecurity risks; and (3) whether and how the board, or relevant body, “considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.” Additionally, the proposed rules would amend Item 407 of Regulation S-K such that registrants would also be required to disclose whether any of its directors have prior work experience, education, or knowledge, skills or other background in cybersecurity.

  Similarly, from a management perspective, the proposed rules would require that registrants disclose whether the registrant has a dedicated CISO, which positions or committees are responsible for detecting, managing, and responding to cybersecurity risk and their corresponding policies and procedures, including the frequency that such committees present to the board on cybersecurity risks.

---

**Key Takeaways**

• **Incident Response Planning.** While the proposed rules clarify that the four-day clock starts from the time that materiality is determined rather than from the time the incident is identified, the facts required to assess the impact of incidents must be timely escalated to the appropriate parties internally to make the materiality
determination. Registrants should review their incident response plans to ensure that they contain an escalation path to the legal and executive teams responsible for assessing materiality.

- **Assess Materiality Thresholds.** The SEC’s commentary makes clear that it understands that materiality is case- and company-specific. Nonetheless, companies should consider leveraging their cybersecurity risk management programs and business continuity programs to evaluate the different cybersecurity risks facing the company and assess the operational, financial, and reputational impact of each type of incident. Understanding the costs of what could go wrong before the incident can help companies establish thresholds for materiality in advance, allowing the company to focus its resources on restoration and mitigation when the incident occurs.

- **Prepare Templates.** While the disclosure in each Item 1.05 8-K will be specific, certain aspects of the disclosure are likely to be the same from incident to incident. Similar to pre-prepared holding statements for customer, investor, or employee communications during an incident, companies should consider what language they can prepare in advance of any incident.

- **Disclosures and Evidence Preservation.** The proposed rules emphasize the importance of clear, accurate, and consistent disclosure regarding cybersecurity risk and incidents to investors and the SEC, formalizing takeaways from the SEC’s 2021 enforcement actions in Pearson and First American. As it has in the past, the SEC will likely use the proposed rules once enacted to scrutinize cybersecurity disclosures and bring enforcement actions concerning deficiencies in cyber disclosures. Companies should ensure that their disclosures are not only accurate, but also are supported by objective evidence and documentation, which will require some thoughtful analysis as to over which aspects of the investigation the company wishes to assert privilege.

- **Test and Train at All Levels.** The proposed rules build on the SEC’s 2018 guidance regarding the board’s involvement in overseeing cybersecurity risk and emphasize the need for both the board and management to understand cybersecurity risk and the steps being taken to mitigate it. As companies continue to test their incident response plans and procedures, companies should consider including both management and the board in tabletop exercises, allowing these key players an opportunity to better understand their roles and responsibilities before, during, and after a cybersecurity incident.

- **De Facto Cybersecurity Standards.** Unlike the SEC’s proposed rules for registered investment advisers, the SEC has not proposed any substantive cybersecurity
requirements for public companies. Despite this, the proposed disclosure requirements are still likely to impact the cybersecurity practices of public companies as the increase in disclosures by registrants will likely reveal common cybersecurity risk mitigation frameworks, practices, and tools. Companies should consider evaluating their cybersecurity programs against known industry standards in anticipation of such public disclosures and take appropriate steps to align their practices.

We will continue to track and blog on these important issues. Public comments are open until at least May 9, 2022.

***

To subscribe to our Data Blog, please click here.

The authors would like to thank Debevoise law clerk Kevin Hayne for his contribution to this post.
On February 9, 2022, the SEC released its much-anticipated proposed rules relating to cybersecurity risk management, incident reporting, and disclosure for investment advisers and funds. Many of the proposals follow the trends that members of the Debevoise Data Strategy & Security and White Collar & Regulatory Defense practice groups discussed during a November 2021 webcast on the SEC’s Cybersecurity Year in Review, as well as in our prior Data Blog posts (here and here).

Chair Gensler recently emphasized that cybersecurity rulemaking in this area is one of his priorities, and placed particular emphasis on establishing standards for cybersecurity hygiene and incident reporting for registrants. The proposed rules, which are the most detailed cybersecurity rules that Chair Gensler’s SEC has issued thus far, reflect the SEC’s intense attention to cybersecurity risk and its willingness to deploy the full scope of its regulatory authority to promulgate standards that address this risk.

These proposed rules would impose significant new requirements on registered investment advisers and funds, and are generally consistent with cybersecurity requirements imposed on other companies by New York’s Part 500 Cybersecurity Regulation and the Federal Trade Commission’s updated Safeguards Rule.

**Key Requirements under the Proposed Rules**

**Cybersecurity Risk Management Policies & Procedures**

The proposed rules would require advisers and funds to adopt and implement policies and procedures that are “reasonably designed” to address cybersecurity risks. There are several “general elements” that advisers and funds will need to address in their cybersecurity policies and procedures, including risk assessment practices, user security and access, preventing unauthorized access to funds, threat and vulnerability management, and incident response and recovery. The proposed rules require advisers and funds, on an annual basis, to: (1) review and assess the design and effectiveness of their cybersecurity policies and procedures; and (2) prepare a report describing the
review, explaining the results, documenting any incident that has occurred since the last report, and discussing any material changes to the policies and procedures since the last report.

The proposed rules also add requirements relating to board oversight and recordkeeping. Under Proposed Rule 38a-2, registered funds would be required to have their boards, including a majority of its independent directors, (1) approve their cybersecurity policies and procedures, and (2) review the annual report.

**Incident Reporting**

The proposed rules would also require advisers, “including on behalf of a client that is a registered investment company or business development company, or a private fund” (collectively, “covered clients”), to report any significant cybersecurity incidents, which are defined as any event that (1) “significantly disrupts or degrades the adviser’s” or private fund client’s “ability to maintain critical operations” or (2) “leads to the unauthorized access or use of adviser information” resulting in substantial harm to the adviser, or substantial harm to a client, or an investor in a private fund, whose information was accessed. Advisers, on behalf of themselves and their covered clients, must report to the SEC within 48 hours from when they have a reasonable basis to believe such an incident has occurred.

Advisers must use the new proposed Form ADV-C for incident notification to the SEC. The notification must include a detailed description of the nature and scope of the incident and any disclosures about it. Advisers will be expected to update any previously submitted Forms ADV-C when there has been a material change in facts. The proposed rule states that submitted Forms ADV-C will remain confidential and not be disclosed to the general public. However, the proposed rules do not address whether the ADV-C filing would be exempt from FOIA.

**Disclosure Obligations for Advisers**

The proposed rules would also amend Form ADV Part 2A for advisers to include disclosure of cybersecurity risks and incidents that could materially affect the advisory relationship with current and prospective clients. The amendment would require that advisers describe, in plain English, the cybersecurity risks that could materially affect the services they offer and how they plan to assess and address those risks. If adopted, the disclosures must include information about the likelihood and extent to which the cybersecurity risk or incident: (1) could occur and what safeguards are in place to prevent it; (2) could or has disrupted the adviser’s ability to provide services; (3) could or has resulted in the loss or compromise of sensitive data; and (4) has or could harm clients.
The proposed amendments would also require advisers to describe any significant cybersecurity incidents that have occurred within the last two fiscal years and require advisers to deliver interim brochure amendments to clients if (1) the adviser was subject to a cybersecurity incident after the dissemination of its brochure, or (2) the information already disclosed in its brochure about an incident materially changes based on new discoveries.

**Disclosure Obligations for Funds**

Under the proposed rules, changes would be made to Forms N-1A, N-2, N-3, N-4, N-6, N-8B-2, and S-6 for funds to report significant cybersecurity incidents and risks, similar to the required disclosures for advisers. The rules propose amendments to funds’ registration forms that would require a description of any significant fund cybersecurity incident that has occurred in its last two fiscal years, and expands the definition of “principal risks” of investing in the fund to include cybersecurity risks and requires disclosure of such in fund registration statements. To the extent that cybersecurity incidents occur after the filing of a fund’s registration forms and this alters the material position or risks involved with the fund, the fund must then file a supplement to the Commission.

**Key Takeaways**

**Prepare for 48-Hour Breach Notice Deadline**

Advisers may find it challenging to meet the strict 48-hour reporting timeline requirements set out by the proposed rules. Many companies have struggled to meet the longer 72-hour breach notification deadlines under the NYDFS Part 500 and GDPR. Having clear protocols for escalating incidents, drafting the notifications, and obtaining the necessary approvals can make the difference between (1) meeting tight notification deadlines and gaining credibility with the applicable regulator, and (2) missing the deadline and starting off having to explain to the regulator why the notification was late, which can undermine the regulator’s view of the overall competence of the response. Advisers can learn from banks that are preparing for the new [36-hour reporting requirement](#), which have started implementing such protocols, including:

- **Who is Covered** -- Determining which entities in their group are subject to the new notification deadline, and if it only applies to some entities, assessing which data, information systems, and employees are associated with the covered entities.

- **Who is Responsible** -- Determining who the person responsible for making the notification, and who else, if anyone, must approve the notification before it is made.
It may be prudent to designate more than one person for each of these roles, in case someone is unavailable.

- **Prompt Escalation** -- Determining which incidents may trigger the short-deadline notification requirement and therefore should be escalated to the persons responsible for that notification, as well as who should be making that escalation.

- **Notification Template** -- Creating a sample notification, so that the actual notification does not need to be drafted from scratch during an incident.

**Adopt, Implement, and Test Policies and Procedures**

The proposed rules expand the policies and procedures obligations for advisers and registered funds. Proposed rules 206(4)-9 and 38a-2 would require advisers and registered funds to establish and implement cybersecurity policies and procedures that are “reasonably designed to mitigate cybersecurity risk,” including risk assessment, standards for user security and access, information protection, threat and vulnerability management, and cybersecurity incident response and recovery. The proposed rules also provide very specific guidance on multiple elements of an expected cybersecurity risk and incident response program; while preexisting policies and procedures may include some of these components, they must now include all of them. Moreover, regular testing to ensure sufficient implementation will be crucial to effective compliance with the SEC’s objectives of cybersecurity risk mitigation and compliance. Targeting policies and procedures violations has been a longstanding enforcement approach for the SEC (see First American), and the proposed rules provide a clear “hook” for doing so in the SEC’s priority area of cybersecurity.

**Disclosures and Evidence Preservation**

The proposed rules emphasize the importance of clear and accurate disclosures regarding cybersecurity risk and incidents to investors and the SEC, formalizing takeaways from the SEC’s 2021 enforcement actions against Pearson and First American as well as the priorities emphasized by Chair Gensler. As it has in the past, we can expect that the SEC will use the proposed rules once enacted to scrutinize cybersecurity-related disclosures and recordkeeping violations through exams and enforcement actions. Companies should ensure that their disclosures are not only accurate, but are also supported by objective evidence and documentation, which will require some thoughtful analysis as to which aspects of the investigation the company wishes to assert privilege.
Incident Response Planning

Through these proposed rules, the SEC has stressed the importance of maintaining continued operations in the event of an incident. Advisers and funds should therefore review their incident response plans and business continuity plans, and consider testing those plans through a tabletop exercises. Given that the proposed rules expand notification obligations of advisers and funds to include incidents affecting private fund and BDC clients’ systems or information, these tabletop exercises can test escalation of incidents and engagement of all the relevant players in the incident response process.

We will continue to track and blog on these important updates. Public comments are open until at least April 9, 2022.

***

The Debevoise Data Portal is now available for clients to help them quickly assess and comply with their state, federal, and international breach notification obligations, as well as their substantive cybersecurity and AI legal obligations.

To subscribe to our Data Blog, please click here.

*The authors would like to thank Linda Lin, a Debevoise law clerk, for her contributions to this post.*

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Charu A. Chandrasekhar
ccrandasekhar@debevoise.com

Matthew C. Rametta
mcrametta@debevoise.com

WASHINGTON, DC

Luke Dembosky
ldembosky@debevoise.com

Julie M. Riewe
jriewe@debevoise.com
On January 24, 2022, SEC Chair Gary Gensler gave a speech on cybersecurity rulemaking to the Annual Securities Regulation Institute, outlining a number of key points he expects the SEC will consider in 2022 and emphasizing the SEC’s “key role” on the federal government’s “Team Cyber.” A number of these proposed changes—including broadening the scope of existing SEC regulations, enhancing SEC requirements for cyber hygiene, and increased attention to public company disclosures—were among the trends that members of the Debevoise Data Strategy & Security and White Collar & Regulatory Defense practice groups discussed during a November 2021 webcast on the SEC’s Cybersecurity Year in Review, as well as in our prior Data Blog posts (here and here).

Below, we highlight a number of key takeaways from Chair Gensler’s speech for SEC-registered entities and public companies.

- **Regulation Systems Compliance and Integrity (“SCI”):** Chair Gensler explained that the SEC would like to “freshen up” Reg SCI, which imposes certain technological and business continuity requirements on the securities market functions of certain large registrants (classified under the Reg as “SCI Entities”) such as stock exchanges, clearinghouses, and alternative trading systems. In particular, Chair Gensler would like to “broaden and deepen” Reg SCI by, for example, bringing more entities (such as large broker-dealers and market makers) within its scope and strengthening certain cyber hygiene requirements.

- **Funds, Advisers, and Broker- Dealers:** Chair Gensler similarly noted that he has already asked his staff how the SEC can “strengthen financial sector registrants’ cybersecurity hygiene and incident reporting” by incorporating guidance from CISA and others. These statements (and Chair Gensler’s comments on customer notifications discussed below) are consistent with our expectation that federal and other regulators are keenly focused on reporting obligations, even if Congress does not pass a general federal data privacy statute. Chair Gensler explained that strengthening reporting would give investors and clients better information,
incentivize good cyber hygiene, and provide the SEC with greater insight into intermediaries' cyber risks.

- **Data Privacy:** The SEC is actively discussing possible updates to Reg S-P. Chair Gensler explained that the SEC is examining how financial sector registrants notify customers and clients of cyber incidents affecting their data and PII. In particular, the SEC is considering changes to the “timing and substance of notifications currently required under Reg S-P[,]” suggesting that the SEC may extend the privacy notice requirements under Reg S-P to cybersecurity events.

- **Public Company Disclosures:** As highlighted by previous enforcement actions such as Pearson Plc, and emphasized in Chair Gensler’s comments, the SEC takes the accuracy and consistency of cybersecurity disclosures seriously. As we noted in our November 2021 webcast, the SEC believes that accurate and complete disclosures regarding cybersecurity risks—and prior actual incidents—are essential. The SEC is currently considering proposed rules that would require enhanced, specific disclosures relating to cybersecurity governance, strategy, and risk management. The proposed rules will likely delineate what is “material” for disclosure purposes after a cyber incident.

- **Service Providers:** Chair Gensler explained that the SEC is considering ways to address cybersecurity risk originating from service providers, including risk disclosure requirements for certain registrants, and even “holding registrants accountable for service providers’ cybersecurity measures,” as it relates to safeguarding investor information. Chair Gensler noted that bank service providers were subject to certain regulation from federal banking regulators, suggesting he saw a similar role for the SEC for vendors of entities within its jurisdiction.

We will continue to track and blog on these important updates.

***

To subscribe to our Data Blog, please click [here](#).

Please do not hesitate to contact us with any questions.
NEW YORK
Avi Gesser
agesser@debevoise.com

NEW YORK
Charu A. Chandrasekhar
cchandrasekhar@debevoise.com

SAN FRANCISCO
Christopher S. Ford
csford@debevoise.com

SAN FRANCISCO
H Jacqueline Brehmer
hjbrehmer@debevoise.com

NEW YORK
Matthew C. Rametta
mcrametta@debevoise.com