# 2022 Annual Conference

May 16 –18 | Washington, DC | Hybrid Event

## Financial and Operational Effective Practices

**Tuesday, May 17, 2022**
**11:00 a.m. – 12:00 p.m.**

This session provides an overview of current financial and operational topics and recent developments in financial and operational rules and requirements applicable to broker-dealers. Join FINRA staff and industry practitioners as they discuss current financial and operational risks and issues impacting firms as well as new and proposed rules. Attendees also learn effective practices taken by compliance and risk professionals to monitor financial and operational risks.

**Moderator:**

Kris Dailey
Vice President, Regulatory Development Services
FINRA Office of Financial and Operational Risk Policy

**Panelists:**

Ann Duguid
Senior Director
FINRA Office of Financial and Operational Risk Policy

Brian Kowalski
Senior Director, Diversified Risk Monitoring
FINRA Member Supervision

Michael Lyons
Chief Financial Officer and Treasurer
National Financial Services

Michael Macchiaroli
Associate Director, Office of Broker-Dealer Finances, Division of Trading and Markets
U.S. Securities and Exchange Commission (SEC)

 

**Financial and Operational Effective Practices Panelists Bios:**

Moderator:

**Kris Dailey** is Vice President in FINRA's Office of Financial and Operational Risk Policy. Ms. Dailey is responsible for leading a team of professionals in developing and interpreting rules and providing policy advice to FINRA staff and member firms. Ms. Dailey's responsibilities span throughout several areas including broker-dealer net capital, liquidity management, accounting and financial reporting obligations, recordkeeping requirements, customer protection requirements, margin requirements and securities clearance and settlement operations, including prime brokerage and financing arrangements. Ms. Dailey's prior roles at FINRA included responsibility for the development of an automated data collection and analysis program in support of FINRA's financial and operational examinations of member firms, assessments of firms' quantitative market and credit risk measurement methodologies and new and continuing membership applications. Before joining FINRA, Ms. Dailey spent more than 15 years at NYSE Regulation, in staff and managerial positions responsible for the examinations and ongoing monitoring of member firms' financial and operational condition. Ms. Dailey received a B.S. in Finance from St. John's University and a M.B.A. from Fordham University.

Panelists:

**Ann Duguid** is Senior Director in the Office of Financial and Operational Risk Policy. In this role, she works closely with FINRA's Member Supervision team providing both accounting policy and financial and operational interpretive guidance related to both introducing and clearing broker dealers. Prior to joining FINRA, Mrs. Duguid worked at J.P. Morgan & Co., where she held various positions, including legal entity controller of J.P. Morgan Securities LLC., regulatory reporting manager (SEA 15c3-1, 15c3-3 and CFTC regulatory reporting), line of business controller for U.S. futures and options clearing and global OTC derivatives brokerage businesses. A Certified Public Accountant with more than 25 years of experience, Ms. Duguid began her career as an auditor at Arthur Andersen & Co. She holds a BBA in Accounting and Management Information Systems from Loyola College in Baltimore, MD.

**Brian Kowalski** is Senior Director and Single Point of Accountability (SPoA) of Risk Monitoring for the Diversified Firm Group within FINRA's Member Supervision Department. In his role, Mr. Kowalski provides strategic leadership and oversees the teams responsible for ongoing risk assessment and monitoring of Medium Diversified firms. He and his team are also responsible for coordination with Examination Program Management on the strategy and execution of related examinations. Prior to this role, Mr. Kowalski was a Surveillance Director within the Risk Oversight and Operational Regulation group of Member Supervision. Mr. Kowalski joined FINRA in 2010 after spending nine years at National Financial Services, LLC in various operations and regulatory control functions.

**Michael Lyons** is Chief Financial Officer and Treasurer of Fidelity's National Financial Services and other Fidelity Brokerage companies. He is co-chair of the FINRA Financial Responsibility Committee, Chair Emeritus of the SIFMA Financial Management Society and a member of the SIFMA Capital and Margin Forum. Mr. Lyons oversees the regulatory and treasury functions for all of Fidelity's broker dealers. Mr. Lyons has been with Fidelity for 16 years and served in various capacities including CFO of Capital Markets and the Operations business units. He also serves as an active member of various not for profit boards and a speaker at various industry conferences. Prior to joining Fidelity, Mr. Lyons was a partner at BDO Seidman in the Financial Services group. He was previously Chief Administrative Officer of U.S. Clearing, a subsidiary of the Quick and Reilly Group, and a Senior Manager at Arthur Andersen. Mr. Lyons earned a BS in Accounting from St. John's University. Mr. Lyons is a CPA and holds Series 27 and 99 licenses.

 

**Michael A. Macchiaroli** is Associate Director of the Office of Broker-Dealer Finances, Division of Trading and Markets for the U.S. Securities and Exchange Commission. He is responsible for the broker-dealer financial responsibility program, which deals with the capital record-keeping, reporting and customer protection Rules. Mr. Macchiaroli has been employed at the Commission since 1970 and in the Division of Trading and Markets since 1978.

 

# Financial and Operational Effective Practices

# Panelists

- **Moderator**
  - Kris Dailey, Vice President, Regulatory Development Services, FINRA FINRA Office of Financial and Operational Risk Policy
- **Panelists**
  - Ann Duguid, Senior Director, FINRA Office of Financial and Operational Risk Policy
  - Brian Kowalski, Senior Director, Diversified Risk Monitoring, FINRA Member Supervision
  - Michael Lyons, Chief Financial Officer and Treasurer, National Financial Services
  - Michael Macchiaroli, Associate Director, Office of Broker-Dealer Finances, Division of Trading and Markets, U.S. Securities and Exchange Commission (SEC)

# Information Notice

# Redesigned eFOCUS System and SEC Security-Based Swap Reporting Requirements; Revised Supplemental Inventory Schedule

June 3, 2021

## Summary

In 2019, the Securities and Exchange Commission (SEC) adopted amendments[1] that revise certain of the Financial and Operational Combined Uniform Single (FOCUS) reporting and annual report requirements that apply to brokers and dealers pursuant to SEA Rule 17a-5[2] to take account of security-based swap (SBS) activity. Further, as a result of these changes, to avoid duplication with the SEC's new requirements, FINRA has revised[3] the Supplemental Inventory Schedule (SIS) so that members that file the new FOCUS Report Part II, pursuant to the SEC's amendments, will no longer need to file the SIS. The SEC's new FOCUS reporting requirements, and the revised SIS, will apply beginning with FOCUS reports and SIS filings that report on the period ending October 31, 2021 and are required to be filed in November 2021. This *Notice* provides highlights of the upcoming changes.

Additionally, FINRA has redesigned its eFOCUS filing system to add certain enhancements and features to improve members' filing experience. Members that are quarterly filers may access the new system on FINRA Gateway beginning June 24, 2021. The new system will be made available to monthly filers beginning in July 2021.

Questions concerning this *Notice* may be directed to:

- Ann Duguid, Senior Director, Office of Financial and Operational Risk Policy, at (646) 315-8434 or Ann.Duguid@finra.org; or
- Jay Koutros, Senior Director, Member Supervision, at (646) 315-8509 or Demetrios.Koutros@finra.org.

### Suggested Routing

- Compliance
- Legal
- Operations
- Regulatory Reporting
- Senior Management

### Key Topic(s)

- Annual Report Filings
- FOCUS Report Filings
- Supplemental Inventory Schedule

### Referenced Rules and Notices

- SEA Rule 17a-5
- Information Notice 11/23/20
- Regulatory Notice 18-38

## Background

In 2019, the SEC, as part of its rulemakings pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act[4] to establish a regulatory framework for SBS, has adopted amendments to the FOCUS reporting and annual report requirements that apply to brokers and dealers. The amendments are designed, among other things, to elicit more detailed information about derivatives positions and exposures. Below are some highlights of how the SEC's amendments impact financial reporting:

- The SEC has amended FOCUS Report Part II. Members that currently file FOCUS Report Part II will file the amended FOCUS Report Part II;
- FOCUS Report Part II CSE will be discontinued. Firms that currently file FOCUS Report Part II CSE will instead file FOCUS Report Part II, as amended;[5]
- Schedule 1 (Aggregate Securities, Commodities and Swaps Positions) of FOCUS Report Part II, as amended, elicits substantially all the information that the current SIS requires. To avoid duplication with Schedule 1 of the SEC's amended FOCUS Report Part II, FINRA has revised the SIS so that members that file FOCUS Report Part II, as amended, will not need to file the SIS;
- The SEC has updated the Facing Page and Oath or Affirmation (Part III of Form X-17A-5), which members submit with their annual reports pursuant to Rule 17a-5. All members will use the amended Facing Page and Oath or Affirmation;
- FOCUS Report Part IIA is unchanged.

The SEC's new FOCUS reporting requirements, and the revised SIS, will apply beginning with FOCUS reports and SIS filings that report on the period ending October 31, 2021 and are required to be filed in November 2021.[6]

Additionally, to improve members' filing experience, FINRA is making available a redesigned eFOCUS system. Members that are quarterly filers may access the new system on FINRA Gateway beginning June 24, 2021. The new system will be made available to monthly filers beginning in July 2021. Members may visit FINRA's eFOCUS page for further information about user support and logging in to the redesigned eFOCUS system. Members with questions about the eFOCUS system may contact the Help Desk at (800) 321-6273.

## Endnotes

1. *See* Securities Exchange Act Release No. 87005 (September 19, 2019), 84 FR 68550 (December 16, 2019) (Final Rule: Recordkeeping and Reporting Requirements for Security-Based Swap Dealers, Major Security-Based Swap Participants, and Broker-Dealers) (referred to as the "Reporting Requirements Release").

2. Rule 17a-5 governs financial and operational reporting by brokers and dealers. Members are required to file with FINRA, through the eFOCUS System, reports concerning their financial and operational status using SEC Form X-17A-5 (the "FOCUS Report"). *See, e.g.,* Information Notice 11/23/20 (2021 and First Quarter of 2022 Report Filing Due Dates); *Regulatory Notice 18-38* (November 2018) (Amendments to the SEC's Financial Reporting Requirements – eFOCUS System Updates and Annual Audit Requirements).

3. See SR-FINRA-2021-013.

4. Pub. L. No. 111-203, 124 Stat. 1376 (2010).

5. Pursuant to the SEC's rulemaking, stand-alone security-based swap dealers (SBSDs) and stand-alone major security-based swap participants (MSBSPs) (that is, SBSDs and MSBSPs that are not broker-dealers and that do not have a prudential regulator) will also file FOCUS Report Part II, as amended. Separately, bank SBSDs and bank MSBSPs (that is, SBSDs and MSBSPs for which there is a prudential regulator) will file new FOCUS Report Part IIC. The SEC, by Order, has designated FINRA as the organization with which stand-alone SBSDs and stand-alone MSBSPs, and bank SBSDs and bank MSBSPs, must file FOCUS Report Part II, as amended, and FOCUS Report Part IIC, respectively. *See* Securities Exchange Act Release No. 88866 (May 14, 2020) (Order Designating Financial Industry Regulatory Authority, Inc., to Receive Form X-17A-5 (FOCUS Report) from Certain Security-Based Swap Dealers and Major Security-Based Swap Participants).

6. This broadly aligns with the October 6, 2021, "compliance date" that the SEC has set for many of its key SBS-related requirements. *See* the Reporting Requirements Release, note 1; *see also* Key Dates for Registration of Security-Based Swap Dealers and Major Security-Based Swap Participants, available on the Commission website.

# Regulatory Notice 21-27

# SEC Financial Responsibility Rules

## FINRA Announces Update of the Interpretations of Financial and Operational Rules

**July 22, 2021**

### Notice Type

- Guidance

### Suggested Routing

- Compliance
- Finance
- Legal
- Operations
- Regulatory Reporting
- Senior Management

### Key Topics

- Customer Protection
- Net Capital

### Referenced Rules & Notices

- SEA Rule 15c3-1
- SEA Rule 15c3-3

## Executive Summary

FINRA is making available updates to interpretations in the Interpretations of Financial and Operational Rules that have been communicated to FINRA by the staff of the SEC's Division of Trading and Markets (SEC staff). The updated interpretations are with respect to Securities Exchange Act (SEA) Rules 15c3-1 and 15c3-3.

Questions concerning this *Notice* should be directed to:

- Yui Chan, Senior Director, Office of Financial & Operational Risk Policy (OFORP), at (646) 315-8426 or Yui.Chan@finra.org;
- Ann Duguid, Senior Director, OFORP, at (646) 315-7260 or Ann.Duguid@finra.org; or
- Kathryn Mahoney, Senior Director, OFORP, at (646) 315-8428 or Kathryn.Mahoney@finra.org.

## Background & Discussion

FINRA is updating interpretations in the Interpretations of Financial and Operational Rules related to SEA Rules 15c3-1 and 15c3-3, as set forth below. Page references are to the hardcopy version. These interpretations are being updated with specific additions, revisions and rescissions.

The following interpretations have been **added**:

- SEA Rule 15c3-1(c)(1)(i)/02 (Indebtedness in the Proprietary Trading Account of a Broker-Dealer) on page 182
- SEA Rule 15c3-1(c)(2)(i)(G)/01 (Services Arrangement with a Parent or an Affiliate) on page 226
- SEA Rule 15c3-1(c)(2)(iv)(B)/16 (Deficits or Unsecured Balances in Securities Transactions with a Federal Reserve Bank) on page 283
- SEA Rule 15c3-1(c)(2)(iv)(C)/095 (Unsecured Receivables and Related Payables) on page 298

- SEA Rule 15c3-1(c)(2)(viii)(C)/033 (Offsetting Sale Commitments in an Unregistered Offering) on page 653
- SEA Rule 15c3-1(e)/01 (Services Arrangement with a Parent or an Affiliate) on page 855
- SEA Rule 15c3-3(j)(2)(ii)(B)(3)(i)(C)/01 (Changing, Adding or Deleting Products Available Through a Sweep Program) on page 2467
- SEA Rule 15c3-3(Exhibit A - Note E(5))/02 (Exclusion of Omnibus Accounts from the Requirements of Note E(5)) on page 2606
- SEA Rule 15c3-3(Exhibit A - General)/012 (Netting a Customer's Account Balances when Preparing the Reserve Formula Computation under the Alternative Standard) on page 2622
- SEA Rule 15c3-3 (Exhibit A - Item 10)/10 (Term Debits in Customers' Accounts Collateralized by Securities Subject to Restrictions on Use) on page 2729

The following interpretations have been **revised**:

- SEA Rule 15c3-1(a)/01 (Additional Net Capital Requirement) on page 1
- SEA Rule 15c3-1(c)(1)/11 (Accrued Liability for Concessions or Commissions Payable) on page 153
- SEA Rule 15c3-1(c)(2)(iv)(C)/091 (Concessions Receivable from Individual Variable Annuities are Allowable for 30 Days; from Group Variable Annuities an Offset is Permitted) on page 296
- SEA Rule 15c3-1(c)(2)(viii)(C)/032 (Offsetting Sale Commitments in a Registered Offering) on page 653
- SEA Rule 15c3-3(a)(1)/01 (Customer/Non-Customer Classification) on page 2003
- SEA Rule 15c3-3 (Exhibit A - Item 10)/07 (Debit Balances in Customers' Accounts Collateralized by Control or Restricted Securities) on page 2728

The following interpretations have been **rescinded**:

- SEA Rule 15c3-1(c)(2)(iv)(C)/09 (Commissions or Concessions Receivable versus Commissions or Concessions Payable) on page 296
- SEA Rule 15c3-3(Exhibit A - Item 11)/041 (Federal Reserve Bank as a Non-Customer) on page 2744

The rule text update is available in portable digital format (pdf) on FINRA's Interpretations of Financial and Operational Rules page.

FINRA member firms and others that maintain the hardcopy version of the Interpretations of Financial and Operational Rules may refer to the accompanying updated page, containing the update, which is being made available to enable the replacement of existing pages in the hardcopy version of the Interpretations of Financial and Operational Rules. The filing instructions for the new page(s) are as follows:

| SEA Rule | Remove Old Pages | Add New Pages |
|---|---|---|
| 15c3-1 | 1 | 1 |
| 15c3-1 | 153 | 153 |
| 15c3-1 | 158 | 158 |
| 15c3-1 | 181-182 | 180-182 |
| 15c3-1 | 225 | 225-226 |
| 15c3-1 | 283 | 283 |
| 15c3-1 | 296-298 | 296-298 |
| 15c3-1 | 653-654 | 653-654 |
| 15c3-1 | 854 | 854-855 |
| 15c3-3 | 2003 | 2003 |
| 15c3-3 | 2467 | 2467 |
| 15c3-3 | 2606 | 2606 |
| 15c3-3 | 2622-2623 | 2622-2623 |
| 15c3-3 | 2727-2729 | 2727-2729 |
| 15c3-3 | 2744 | 2744 |

Further, the SEC staff continues to communicate and issue written and oral interpretations of the financial responsibility and reporting rules. FINRA will update the Interpretations of Financial and Operational Rules on its website as these written and oral interpretations are issued.

# Regulatory Notice 21-29

# Vendor Management and Outsourcing

## FINRA Reminds Firms of their Supervisory Obligations Related to Outsourcing to Third-Party Vendors


### Summary

Member firms are increasingly using third-party vendors to perform a wide range of core business and regulatory oversight functions. FINRA is publishing this *Notice* to remind member firms of their obligation to establish and maintain a supervisory system, including written supervisory procedures (WSPs), for any activities or functions performed by third-party vendors, including any sub-vendors (collectively, Vendors) that are reasonably designed to achieve compliance with applicable securities laws and regulations and with applicable FINRA rules. This *Notice* reiterates applicable regulatory obligations; summarizes recent trends in examination findings, observations and disciplinary actions; and provides questions member firms may consider when evaluating their systems, procedures and controls relating to Vendor management.


This *Notice*—including the "Questions for Consideration" below—does not create new legal or regulatory requirements or new interpretations of existing requirements. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their Vendor management practices. FINRA recognizes that there is no one-size-fits-all approach to Vendor management and related compliance obligations, and that firms use risk-based approaches that may involve different levels of supervisory oversight, depending on the activity or function Vendors perform. Firms may consider the information in this *Notice* and employ the practices that are reasonably designed to achieve compliance with relevant regulatory obligations based on the firm's size and business model.

FINRA also notes that the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency recently published and requested comment on proposed guidance designed to help banking organizations manage risks associated with third-party relationships. FINRA will monitor this proposed guidance and consider comparable action, where appropriate.

**August 13, 2021**

### Notice Type

- Guidance

### Suggested Routing

- Business Senior Management
- Compliance
- Cyber
- Information Technology
- Legal
- Operations
- Risk Management

### Key Topics

- Business Continuity Planning (BCP)
- Cybersecurity
- Due Diligence
- Internal Controls
- Supervision
- Vendor Management

### Referenced Rules & Notices

- FINRA Rule 1220
- FINRA Rule 3110
- FINRA Rule 4311
- FINRA Rule 4370
- Regulation S-P Rule 30
- Notice to Members 05-48

Questions or comments concerning this *Notice* may be directed to:

- Ursula Clay, Senior Vice President and Chief of Staff, Member Supervision, at 646-315-7375 or Ursula.Clay@finra.org;
- Sarah Kwak, Associate General Counsel, Office of General Counsel, at 202-728-8471 or Sarah.Kwak@finra.org;
- Michael MacPherson, Senior Advisor, Member Supervision, at 646-315-8449 or Michael.MacPherson@finra.org.

## Background and Discussion

In 2005, FINRA published *Notice to Members 05-48* (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers), which identified a number of common activities or functions that member firms frequently outsourced to Vendors, including "accounting/finance (payroll, expense account reporting, etc.), legal and compliance, information technology (IT), operations functions (*e.g.,* statement production, disaster recovery services, etc.) and administration functions (*e.g.,* human resources, internal audits, etc.)." Since that time, including during the COVID-19 pandemic, member firms have continued to expand the scope and depth of their use of technology and have increasingly leveraged Vendors to perform risk management functions and to assist in supervising sales and trading activity and customer communications.[1]

FINRA encourages firms that use—or are contemplating using—Vendors to review the following obligations and assess whether their supervisory procedures and controls for outsourced activities or functions are sufficient to maintain compliance with applicable rules.

| CATEGORY | SUMMARY OF REGULATORY OBLIGATIONS |
|---|---|
| **Supervision** | FINRA Rule 3110 (Supervision) requires member firms to establish and maintain a system to supervise the activities of their associated persons that is reasonably designed to achieve compliance with federal securities laws and regulations, as well as FINRA rules, including maintaining written procedures to supervise the types of business in which it engages and the activities of its associated persons.<br><br>This supervisory obligation extends to member firms' outsourcing of certain "covered activities"—activities or functions that, if performed directly by a member firm, would be required to be the subject of a supervisory system and WSPs pursuant to FINRA Rule 3110.[2]<br><br>*Notice* 05-48 reminds member firms that "outsourcing an activity or function to ... [a Vendor] does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and [FINRA] and MSRB rules regarding the outsourced activity or function." Further, *Notice* 05-48 states that if a member outsources certain activities, "the member's supervisory system and [WSPs] must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and [FINRA] rules."<br><br>FINRA expects member firms to develop reasonably designed supervisory systems appropriate to their business model and scale of operations that address technology governance-related risks, such as those inherent in firms' change and problem-management practices. Failure to do so can expose firms to operational failures that may compromise their ability to serve their customers or comply with a range of rules and regulations, including FINRA Rules 4370 (Business Continuity Plans and Emergency Contact Information), 3110 (Supervision) and books and records requirements under 4511 (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4. |

| CATEGORY | SUMMARY OF REGULATORY OBLIGATIONS |
|---|---|
| **Registration** | *Notice* 05-48 reminds firms that, "in the absence of specific [FINRA] rules, MSRB rules, or federal securities laws or regulations that contemplate an arrangement between members and other registered broker-dealers with respect to such activities or functions (*e.g.,* clearing agreements executed pursuant to [FINRA Rule 4311]), any third-party service providers conducting activities or functions that require registration and qualification under [FINRA] rules will generally be considered associated persons of the member and be required to have all necessary registrations and qualifications."<br><br>Accordingly, firms must review whether Vendors or their personnel meet any registration requirements under FINRA Rule 1220 (Registration Categories), as well as whether employees of the member firm are "Covered Persons" under the Operations Professional registration category pursuant to FINRA Rule 1220(b)(3), due to their supervision of "Covered Functions" executed by a Vendor or because they are authorized or have the discretion materially to commit the member firm's capital in direct furtherance of a Covered Function or to commit the member firm to any material contract or agreement (written or oral) with a Vendor in furtherance of a Covered Function. |
| **Cybersecurity** | SEC Regulation S-P Rule 30 requires broker-dealers to have written policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information that are reasonably designed to: (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.<br><br>FINRA expects member firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations. FINRA reminds member firms to review core principles and effective practices for developing such programs and controls, including Vendor management, from our Report on Cybersecurity Practices (2015 Report) and the Report on Selected Cybersecurity Practices – 2018 (2018 Report), as well as other resources included in the Appendix to this *Notice*. |

| CATEGORY | SUMMARY OF REGULATORY OBLIGATIONS |
|---|---|
| **Business Continuity Planning (BCP)** | FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires member firms to create and maintain a written BCP with procedures that are reasonably designed to enable member firms to meet their existing obligations to customers, counterparties and other broker-dealers during an emergency or significant business disruption. The elements of each member firm's BCP—including their use of Vendors—can be "flexible and may be tailored to the size and needs of a member [firm]," provided that minimum enumerated elements are addressed. As a reminder, member firms must review and update their BCPs, if necessary, in light of changes to member firms' operations, structure, business or location. |

## Exam Findings and Observations

The 2021 Report on FINRA's Exam and Risk Monitoring Program, as well as our 2019, 2018 and 2017 Reports on FINRA Examination Findings, addressed compliance deficiencies (discussed below) arising from firms' Vendor relationships.

## Cybersecurity and Technology Governance

- **Vendor Controls** – Firms failed to document or implement procedures to: 1) evaluate prospective and, as appropriate, test existing Vendors' cybersecurity controls, or 2) manage the lifecycle of their engagement with Vendors (*i.e.,* from onboarding, to ongoing monitoring, through off-boarding, including defining how Vendors dispose of customer non-public information).
- **Access Management** – Firms failed to implement effective Vendor access controls, including: limiting and tracking Vendors with administrator access to firm systems; instituting controls, such as a "policy of least privilege," to grant system and data access to Vendors only when required and removing access when no longer needed; or implementing multi-factor authentication for Vendors and contractors.
- **Inadequate Change Management Supervision** – Firms did not perform sufficient supervisory oversight of Vendors' application and technology changes impacting firm business and compliance processes, especially critical systems (including upgrades, modifications to or integration of member firm or Vendor systems). These oversight failures led to violations of regulatory obligations, such as those relating to data integrity, cybersecurity, books and records and confirmations.
- **Limited Testing of System Changes and Capacity** – Firms did not adequately test changes to, or system capacity of, order management, account access and trading algorithm systems, and thus failed to detect underlying malfunctions or capacity constraints.
- **Data Loss Prevention Programs** – Vendors did not encrypt confidential firm and customer data (*e.g.,* Social Security numbers) stored at Vendors or in transit between firms and Vendors.

### FINRA Disciplined Firms Whose Vendors Did Not Implement Technical Controls

FINRA disciplined certain firms for violations of Regulation S-P Rule 30 and FINRA Rules 3110 and 2010 for failing to maintain adequate procedures and execute supervisory oversight to protect the confidentiality of their customers' nonpublic personal information, including, for example, where:

- a Vendor exposed to the public internet the firms' purchase and sales blotters, which included customers' nonpublic personal information (*e.g.,* names, account numbers, and social security numbers).
- a Vendor did not configure its cloud-based server correctly, install antivirus software, and implement encryption for the firm's account applications and other brokerage records containing customers' nonpublic personal information. As a result, foreign hackers successfully accessed the cloud-based server and exposed firm customers' nonpublic personal information.

## Books and Records

- Firms failed to perform adequate due diligence to verify Vendors' ability to maintain books and records on behalf of member firms in compliance with 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).
- Firms failed to confirm that service contracts and agreements comply with requirements to provide notification to FINRA under Exchange Act Rule 17a-4(f)(2)(i), including a representation that the selected electronic storage media (ESM) used to maintain firms' books and records 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).
- Firms did not confirm that Vendors complied with contractual and regulatory requirements to maintain (and not delete, unless otherwise permitted) firms' books and records.[3]

**Consolidated Account Reports (CARs)** – Firms did not have processes in place to evaluate how they and registered representatives selected CARs Vendors; set standards for whether and when registered representatives were authorized to use Vendor-provided CARs; determine when and how registered representatives could add manual entries or make changes to CARs; test or otherwise validate data for non-held assets reported in CARs (or clearly and prominently disclose that the information provided for those assets was unverified); and maintain records of CARs.[4]

**Fixed Income Mark-up Disclosure** – Firms failed to test whether Vendors identified the correct prevailing market price (PMP) from which to calculate mark-ups and mark-downs (for example, instead of using the prices of a member firm's own contemporaneous trades, which were available to be considered, a Vendor's program incorrectly identified PMPs using lower levels of the "waterfall" as described in FINRA Rule 2121.02 (Additional Mark-Up Policy For Transactions in Debt Securities, Except Municipal Securities) or MSRB Rule G-30.06 (Mark-Up Policy).

### FINRA Disciplined Firms for Books and Records Violations Resulting from Vendor Deficiencies

FINRA disciplined firms for violations of Books and Records rules and related supervisory obligations involving Vendors, including, but not limited to, failing to preserve and produce business-related electronic communications (including emails, social media, texts, instant messages, app-based messages and video content) due to:

- Vendors' system malfunctions;
- Vendors' data purges after termination of their relationship with firms;
- Vendors failing to correctly configure default retention periods resulting in inadvertent deletions of firm electronic communication for certain time periods;
- Vendors' system configurations making deleted emails unrecoverable after 30 days;
- Vendors failing to provide non-rewriteable, non-erasable storage; and
- Firms failing to establish an audit system to account for Vendors' preservation of emails.

## Questions for Consideration

The following questions may help firms evaluate whether their supervisory control system, including WSPs, adequately addresses issues and risks relating to Vendor management. The questions—which address both regulatory requirements and effective practices FINRA has observed firms implement—focus on four phases of a firm's outsourcing activities:

- deciding to outsource an activity or function,
- conducting due diligence on prospective Vendors,
- onboarding Vendors, and
- overseeing or supervising outsourced activities or functions.

As noted above, firms should not infer any new obligations from the questions for consideration. Many of the reports, tools or methods described herein reflect information firms have told FINRA they find useful in their vendor management practices. FINRA is sharing this information for firms' consideration only.

Firms may wish to evaluate the questions presented below in the context of a risk-based approach to Vendor management in which the breadth and depth of their due diligence and oversight may vary based on the activity or function outsourced to a Vendor. Factors firms may take into consideration include, but are not limited to:

- Will the Vendor be handling sensitive firm or customer non-public information?
- What would be the extent of the potential damage if there is a security breach (*e.g.,* number of customers or prospective customers impacted)?
- Is the Vendor performing a business-critical role or fulfilling a regulatory requirement for the firm?
- What is the reputation and history of the Vendor, including the representations made and information shared on how the Vendor will secure the firm's information?

**I. Decision to Outsource**

A decision to outsource an activity or function may depend, in part, on whether the firm has an adequate process to make that determination and then to supervise that outsourced activity or function. The following considerations may help firms address those threshold questions.

- Does your firm have a process for its decision-making on outsourcing, including the selection of Vendors?
- Does your firm's supervisory control system address your firm's outsourcing practices, including your firm's approach to Vendor due diligence?
- Does your firm identify risks that may arise from outsourcing a particular activity or function and consider the impact of such outsourcing on its ability to comply with federal securities laws and regulations, and FINRA rules?
- Does your firm engage key internal stakeholders (*e.g.,* Compliance, Legal, IT or Risk Management) relevant to, and with the requisite experience to assess, the outsourcing decision?

**II. Due Diligence**

Once a member firm decides to outsource an activity or function, it may want to consider some or all of the following questions in evaluating and selecting potential Vendors:

- Due Diligence Approach
  - What factors does your firm consider when conducting due diligence on potential Vendors? These may include, but are not limited to: a Vendors' financial condition, experience and reputation; familiarity with regulatory requirements, fee structure and incentives; the background of Vendors' principals, risk management programs, information security controls, and resilience.

- If a potential Vendor will be performing a function that is subject to regulatory requirements, how does your firm evaluate whether the Vendor has the ability to comply with applicable regulatory requirements and undertakings (*e.g.,* Book and Records rules, including ESM Notification Requirements)?
- Does your firm consider obtaining evaluations of prospective Vendors' SSAE 18, Type II, SOC 2 (System and Organization Control) reports (if available)? If so, who reviews the evaluations and how does your firm follow up on any identified concerns, including, for example, those related to cybersecurity?
- Does your firm take a risk-based approach to vendor due diligence? Does the scope and depth of your firm's due diligence reflect the degree of risk associated with the activities or functions that will be outsourced?
- Does your firm evaluate the impact to your customers or firm if a Vendor fails to perform, for example, by not fulfilling a regulatory obligation? What measures can your firm put in place to mitigate that risk?
- Does your firm assess the BCPs of prospective Vendors that would perform critical business, operational, risk management or regulatory activities or functions?
- If a Vendor will likely be conducting activities or functions that require registration under FINRA rules, does your firm have a process for determining whether the Vendor's personnel will be appropriately qualified and registered?
- Does your firm evaluate Vendors' controls and due diligence of Vendors' sub-contractors, particularly if the sub-contractor may have access to sensitive firm or customer non-public information or critical firm systems?
- Does your firm include individuals with the requisite expertise and experience in the due diligence process—including with respect to cybersecurity, information technology, risk management, business functions and relevant regulatory obligations—to effectively evaluate potential Vendors? How does your firm handle instances where your firm does not have the expertise or experience in-house?
- Does your firm document its due diligence findings?

- **Conflicts of Interest –** Does your firm put controls in place to mitigate potential conflicts of interest in the Vendor selection process? For example:
  - Does your firm require staff involved in its Vendor selection processes to disclose any personal relationship with the Vendor? If so, what steps does your firm take to assess whether that relationship may influence the choice of Vendor?
  - Does your firm allow staff to receive compensation or gifts from potential or current Vendors, which could influence the decision to select, or maintain a relationship with, a particular Vendor?

- **Cybersecurity**

Does your firm assess the Vendors' ability to protect sensitive firm and customer non-public information and data? Does your firm have access to expertise to conduct that assessment? (See also question, above, regarding SSAE 18 Type II, SOC 2 reports.)

### III. Vendor Onboarding

After completing due diligence and selecting a Vendor, firms may wish to consider putting in place a written contract with the Vendor that addresses, among other things, both the firm's and the Vendor's roles with respect to outsourced regulatory obligations.

- **Vendor Contracts**
  - Does your firm document relationships with Vendors in a written contract, and if not, under what circumstances?
  - Do your firm's contracts address, when applicable, Vendors' obligations with respect to such issues as:
    - documentation evidencing responsible parties' and Vendors' compliance with federal and state securities laws and regulations and FINRA rules (*e.g.,* retention period required for preservation of firm records);
    - non-disclosure and confidentiality of information;
    - protection of non-public, confidential and sensitive firm and customer information;
    - ownership and disposition of firm and customer data at the end of the Vendor relationship;
    - notification to your firm of cybersecurity events and the Vendor's efforts to remediate those events, as well as notification of data integrity and service failure issues;
    - Vendor BCP practices and participation in your firm's BCP testing, including frequency and availability of test results;
    - disclosure of relevant pending or ongoing litigation;
    - relationships between Vendors, sub-contractors and other third-parties;
    - firm and regulator access to books and records; and
    - timely notification to your firm of application or system changes that will materially affect your firm.
  - Do your firm's contracts with Vendors address roles, responsibilities and performance expectations with respect to outsourced activities or functions?

- **Features and Default Settings of Vendor Tools**
  - Does your firm review, and as appropriate adjust, Vendor tool default features and settings, such as to limit use of communication tools to specific firm-approved features (*e.g.,* disabling a chat feature, or reviewing whether the communications are being captured for supervisory review), to set the appropriate retention period for data stored on a vendor platform or to limit data access—to meet your firm's business needs and applicable regulatory obligations?

**IV. Supervision**

Member firms have a continuing responsibility to oversee, supervise and monitor the Vendor's performance of the outsourced activity or function. Firms may wish to consider the following potential steps in determining how they fulfill this supervisory obligation:

- Obtaining representations from the Vendor in a contractual agreement that they are conducting self-assessments and undertaking the specific responsibilities identified;
- Requiring Vendors to provide attestations or certifications that they have fulfilled certain reviews or obligations;
- Going onsite to Vendors to conduct testing or observation, depending on the firm's familiarity with the vendor or other risk-based factors;
- Monitoring and assessing the accuracy and quality of the Vendor's work product;
- Remaining aware of news of Vendor deficiencies and investigating whether they are indicative of a problem with an activity or function the Vendor is performing for your firm;
- Investigating customer complaints that may be indicative of issues with a Vendor and exploring whether there are further-reaching impacts; and
- Training staff to address and escalate red flags at your firm that a Vendor may not be performing an activity or function adequately, such as not receiving confirmation that a Vendor task was completed.

In addition to the above, firms may want to consider asking the following questions, where applicable, with respect to more specific aspects of their supervisory system.

- **Supervisory Control System**
  - Does your firm monitor Vendors (for example, by reviewing SOC 2 reports) and document results of its ongoing supervision, especially for critical business or regulatory activities or functions?
  - Do your firm's WSPs address roles and responsibilities for firm staff who supervise Vendor activities?
  - Does your firm periodically review and update its Vendor management-related WSPs to reflect material changes in the firm's business or business practices?

- **Business Continuity Planning**
  - Does your firm's business continuity planning and testing include Vendors? If so, what are the testing requirements for Vendors and how often are such tests performed? How do these tests inform your firm's overall BCP?
  - Does your firm have contingency plans for interruptions or terminations of Vendor services?
  - If there is a disaster recovery event, has your firm assessed whether the Vendor will have sufficient staff dedicated to your firm?
- **Cybersecurity and Technology Change Controls**
  - **Access Controls**
    - Does your firm know which Vendors have access to: (1) sensitive firm or customer non-public information and (2) critical firm systems?
    - Does your firm implement access controls through the lifecycle of its engagement with Vendors, including developing a "policy of least privilege" to grant Vendors system and data access only when required and revoke it when no longer needed and upon termination?
    - Has your firm considered implementing multi-factor authentication for Vendors and, if warranted, their sub-contractors?
  - **Cybersecurity Events and Data Breaches**
    - Does your firm conduct independent, risk-based reviews to determine if Vendors have experienced any cybersecurity events, data breaches or other security incidents? If so, does your firm evaluate the Vendors' response to such events?
    - If a cybersecurity breach occurred at your firm's Vendor, was your firm notified and, if so, how quickly? Did your firm follow its incident response plan for addressing such breaches?
  - **Technology Change Management**
    - If applicable, how does your firm become aware of, evaluate and, as appropriate, test the impact of changes Vendors make to their applications and systems, especially for critical applications and systems?

### FINRA Disciplined Firms for Failure to Supervise Vendors

FINRA disciplined certain firms that violated FINRA Rules 2010 and 3110, among other rules, when they failed to establish and maintain supervisory procedures for their Vendor arrangements reasonably designed to:

- Review, verify or correct vendor-provided expense ratio and historical performance information for numerous investment options in defined contribution plans (*i.e.,* retirement plans), causing firms' customer communications to violate FINRA Rule 2210;
- Oversee, monitor and evaluate changes and upgrades to automated rebalancing and fee allocation functions outsourced to a Vendor for wealth management accounts custodied at the firm, causing errors and imposing additional fees to customer accounts;
- Review, test or verify the accuracy and completeness of data feeds from Vendors that failed to identify the firm's prior role in transactions for issuers covered by firm research reports, resulting in violations of then NASD Rule 2711(h) and 2241(c) when the firm failed to make required disclosures in its equity research reports regarding its status as a manager or a co-manager of a public offering of the issuer's equity securities; and
- Confirm the accuracy and completeness of information provided by Vendors to regulators, including FINRA, both in response to specific requests and as part of regular trade and other reporting obligations, causing inaccurate responses and misreported transactions, order reports, route reports and reportable order events.

## Conclusion

As noted throughout this *Notice*, the requirement that a member firm maintain a reasonably designed supervisory system and associated WSPs extends to activities or functions it may outsource to a Vendor. While the manner and frequency by which these activities or functions are overseen is determined by the member firm, and is dependent on a number of factors, the information in this *Notice* is intended to provide firms with ideas and questions they can use to build and evaluate the sufficiency of their Vendor management protocols. Additional helpful resources can be found in the Appendix.

## Endnotes

1. *See Regulatory Notice* 20-42 (FINRA Seeks Comment on Lessons from the COVID-19 Pandemic); COVID-19/Coronavirus Topic Page; *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); and *Regulatory Notice* 20-08 (Pandemic-Related Business Continuity Planning, Guidance and Relief).

2. *See also* NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance, which clarified that *Notice 05-48* was issued to provide guidance on a member's responsibilities if the member outsources certain activities and was not intended to address the appropriateness of outsourcing a particular activity or whether an activity could be outsourced to a non-broker-dealer third-party service provider.

3. *See Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services).

4. *See Regulatory Notice* 10-19 (FINRA Reminds Firms of Responsibilities When Providing Customers with Consolidated Financial Account Reports).

# Appendix – Additional Resources

## Regulatory Notices and Guidance

- **Outsourcing and Vendor Management**
  - *Regulatory Notice* 11-14 (FINRA Requests Comment on Proposed New FINRA Rule 3190 to Clarify the Scope of a Firm's Obligations and Supervisory Responsibilities for Functions or Activities Outsourced to a Third-Party Service Provider)
  - *Notice to Members* 05-48 (Members' Responsibilities When Outsourcing Activities to Third-Party Providers), and NASD Office of General Counsel, Regulatory Policy and Oversight Interpretive Guidance
  - *Regulatory Notice* 18-31 (SEC Staff Issues Guidance on Third-Party Recordkeeping Services)
- **Cybersecurity**
  - Report on Selected Cybersecurity Practices – 2018
  - Report on Cybersecurity Practices – 2015

## FINRA Examination Findings Reports

- 2021 Report on FINRA's Examination and Risk Monitoring Program
- 2019 Report on FINRA Examination Findings and Observations
- 2018 Report on FINRA Examination Findings
- 2017 Report on FINRA Examination Findings

## Tools

- Core Cybersecurity Controls for Small Firms
- Small Firm Cybersecurity Checklist
- Outsourcing and Vendor Management section of the Peer-2-Peer Compliance Library
  - Outsourcing Due Diligence Form
  - Sample Vendor On-Site Audit Template
  - Sample Vendor Questionnaire
  - Third Party Matrix
  - Third Party Vendor Contracts Sample Language
  - Vendor Management Considerations
  - Vendor Security Questionnaire