Vendor Management: Due Diligence and Oversight
Tuesday, May 17, 2022
8:30 a.m. – 9:30 a.m.

During this session, FINRA staff walk through various important considerations when choosing new vendors. Panelists discuss finding a technical solution that is a good fit for your firm, tips on performing an efficient due diligence review, contract issues, and advice on implementing the new software.

Moderator:
Kyle Morse
Vice President, Trading and Execution (T&E) Firm Examinations
FINRA Market Regulation

Panelists:
Catherine Dunn
Director, Capital Markets Firm Examinations
FINRA Member Supervision

Yuliana Landers
Manager, Retail Firm Examinations
FINRA Member Supervision

Matthew Reyburn
Director, Capital Markets Risk Monitoring
FINRA Member Supervision

Vendor Management: Due Diligence and Oversight Panelists Bios:

Moderator:

Kyle Morse, Vice President, Trading and Execution (T&E), currently manages examination teams for Market Regulation covering FINRA Firm Exams as well as Exchange RSA Sales Practice and T&E Fixed Income Trading Exams. Prior to assuming his role in the T&E examination program, Mr. Morse managed surveillance and investigative teams in Market Regulation for both Quality of Markets and Options Regulation. He has been with FINRA for 17 years and previously worked as a regulator for NYSE Arca, Pacific Stock Exchange and the Chicago Stock Exchange. Mr. Morse is currently the Executive Sponsor for the FINRA Women's Network. Outside of FINRA, Mr. Morse volunteers his time with the Cystic Fibrosis Foundation, serving as the President of the Corporate Advisory Board and Co-Chair of the Outreach and Advocacy Committee. Mr. Morse earned his B.A. from Illinois State University and his M.B.A in Financial Analysis from DePaul University.

Panelists:

Catherine Dunn is Examination Director in the Capital Markets Firm Examination Group within FINRA's Member Supervision Department. Ms. Dunn has been in this role since June 2020 and is based in the New Jersey Office. In this position, Ms. Dunn is responsible for leading a team of Examination Managers and Examiners who execute firm examinations. Ms. Dunn was an Examination Manager for 19 years in the New Jersey Office and has been associated with FINRA's Examination Program since joining FINRA in1999. Previously, Ms. Dunn worked at Merrill Lynch as a Senior Accountant in Financial Reporting and as an Auditor in the banking industry. Ms. Dunn has a B.S. in Accounting from Rutgers University.

Yuliana Landers is Examination Manger for FINRA's Member Supervision examination program. In this capacity, she has responsibility for managing a team that executes examinations of member firms who primarily service retail customers. Throughout her 10-year tenure at FINRA, Ms. Landers has held positions ranging from Compliance Examiner to Examination Manager. Ms. Landers began her career in Consumer and Small Business Banking with Wells Fargo Bank before obtaining her FINRA Series 7 and 66 licenses and transitioning to Wells Fargo Advisors. She received her Bachelor of Arts in Economics from Wartburg College and her Master of Science in Finance from University of Colorado. She is a member of the Association of Certified Anti-Money Laundering Specialists and serves as a Director for the Cancer League of Colorado Foundation.

Matt Reyburn is Risk Monitoring Director for the FINRA Capital Markets and Investment Banking firm grouping. During his 19 years with FINRA, he has served various roles as an Examiner and Examination Manager prior to becoming a Risk Monitoring Director. Mr. Reyburn's experience includes performing examination work through regulatory services agreements for the NASDAQ-LIFFE Single Stock Futures Exchange and Chicago Climate Exchange. As a Risk Monitoring Director, Mr. Reyburn and his team of analysts are responsible for performing the sales practice and financial/operational monitoring of approximately 270 Mergers and Acquisition broker-dealers located across the nation. Prior to joining FINRA, Mr. Reyburn performed various roles including Examination Manager and Strategic Development Analyst at the National Futures Association.

Vendor Management: Due Diligence and Oversight

Panelists

- **Moderator**
  - Kyle Morse, Vice President, Trading and Execution (T&E) Firm Examinations, FINRA Market Regulation
- **Panelists**
  - Catherine Dunn, Director, Capital Markets Firm Examinations, FINRA Member Supervision
  - Yuliana Landers, Manager, Retail Firm Examinations, FINRA Member Supervision
  - Matthew Reyburn, Director, Capital Markets Risk Monitoring, FINRA Member Supervision

To Access Polling

- **Please get your devices out:**
  - Type the polling address, **https://finra.cnf.io/sessions/ey7n** into the browser or scan the QR code with your camera.

  - Select your polling answers.

Polling Question 1

1. **Approximately how many services/functions does your firm outsource to a third-party?**
   a. 0
   b. 1-5
   c. 6-10
   d. 10+

Polling address: **https://finra.cnf.io/sessions/ey7n**

Polling Question 2

2. Approximately how many of your vendors does your firm maintain a written contract with?
   a. 0
   b. <25%
   c. 25-50%
   d. 50-75%
   e. 75%+

Polling address: **https://finra.cnf.io/sessions/ey7n**

Polling Question 3

3. **Is your off-boarding process documented in your firm's procedures and/or contracts with vendors?**
   a. Procedures
   b. Contracts
   c. Both
   d. Neither

Polling address: **https://finra.cnf.io/sessions/ey7n**

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. 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] *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." 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." 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. 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

Notice to Members

JULY 2005

SUGGESTED ROUTING

Legal and Compliance
Operations
Senior Management

KEY TOPICS

Due Diligence
Outsourcing
Supervisory Responsibilities
Third-Party Service Providers

GUIDANCE

Outsourcing

Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers

Executive Summary

NASD is aware that members are increasingly contracting with third-party service providers to perform certain activities and functions related to their business operations and regulatory responsibilities that members would otherwise perform themselves—a practice commonly referred to as outsourcing. NASD is issuing this *Notice* to remind members that, in general, any parties conducting activities or functions that require registration under NASD rules will be considered associated persons of the member, absent the service provider separately being registered as a broker-dealer and such arrangements being contemplated by NASD rules (such as in the case of clearing arrangements), MSRB rules, or applicable federal securities laws or regulations. In addition, outsourcing an activity or function to a third party does not relieve members of their ultimate responsibility for compliance with all applicable federal securities laws and regulations and NASD and MSRB rules regarding the outsourced activity or function. As such, members may need to adjust their supervisory structure to ensure that an appropriately qualified person monitors the arrangement. This includes conducting a due diligence analysis of the third-party service provider.

Questions/Further Information

Questions or comments concerning this *Notice* may be directed to Patricia Albrecht, Assistant General Counsel, Office of General Counsel, Regulatory Policy and Oversight, at (202) 728-8026.

Background

The practice of contracting with third-party service providers/vendors to perform certain activities and functions on a continuing basis (outsourcing) is not new to the securities industry. For example, NASD Rule 3230 (Clearing Agreements) has long permitted members that are introducing broker-dealers to enter into contracts with registered clearing broker-dealers that allocate certain functions and responsibilities, such as providing execution services, custody, and margin; maintaining books and records; and receiving, delivering, and safeguarding funds. Over the years, however, members' outsourcing activities have grown beyond the use of clearing agreements. Now, members regularly enter into outsourcing arrangements with entities other than broker-dealers. These entities may be unregulated, such as providers of data services, or regulated, such as transfer agents. Additionally, members increasingly are outsourcing activities other than those traditionally performed pursuant to clearing agreements.

To better understand their members' outsourcing activities, NASD and the New York Stock Exchange (NYSE) conducted a joint survey in October 2004 of a select number of broker-dealers. The survey sought to determine whether broker-dealers had procedures in place to determine the proficiency of service providers, whether outsourced business functions were properly monitored, and whether broker-dealers were in compliance with applicable regulations pertaining to the privacy of customer information in connection with such outsourcing arrangements. The survey found that, in many instances, there was a lack of written procedures to monitor the outsourcing of services, a lack of business continuity plans on the part of service providers and members with respect to outsourced services, and a lack of formalized due diligence processes to screen service providers for proficiency. However, while not always in the form of written procedures, most participants reported that they did have methods that they used to monitor and assess a third-party vendor's own procedures and performance and the accuracy and quality of the work product produced on a continuing basis. These methods included (1) using programmatic checks through business operations; (2) including the procedures in the contracts with the vendors; (3) requiring status reports and periodic meetings; and (4) testing and reviewing the third parties' procedures.

The survey results also provided a snapshot of the type and range of activities being outsourced and the nature of the third-party service providers being used. Survey participants frequently outsourced functions associated with 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.). Approximately two-thirds of the third-party vendors used by survey participants were regulated entities, subject to the jurisdiction of the Securities and Exchange Commission, NASD, NYSE, the Board of Governors of the Federal Reserve System, and/or the Office of the Comptroller of the Currency. The remaining third-party vendors were unregulated entities—both foreign and domestic. Survey participants indicated that they used foreign third-party vendors most often when outsourcing IT and communications activities.[1]

Discussion

Given the growing trend among members to outsource an increasing number of activities and functions to outside entities—both regulated and unregulated—and the lack of uniformity in members' procedures regarding members' use of outsourcing, NASD is issuing this *Notice* to provide guidance on requirements that pertain to the outsourcing of activities and functions that, if performed directly by members, would be required to be the subject of a supervisory system and written supervisory procedures pursuant to Rule 3010 (covered activities).[2] In addition, members are reminded that, in the absence of specific NASD 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 NASD Rule 3230), any third-party service providers conducting activities or functions that require registration and qualification under NASD rules will generally be considered associated persons of the member and be required to have all necessary registrations and qualifications.

I. Accountability and Supervisory Responsibility for Outsourced Functions

Rule 3010 requires NASD members to design a supervisory system and corresponding written supervisory procedures that are appropriately tailored to each member's business structure.[3] If a member, as part of its business structure, outsources covered activities, the member's supervisory system and written supervisory procedures must include procedures regarding its outsourcing practices to ensure compliance with applicable securities laws and regulations and NASD rules. The procedures should include, without limitation, a due diligence analysis of all of its current or prospective third-party service providers to determine whether they are capable of performing the outsourced activities.[4]

After the member has selected a third-party service provider, the member has a continuing responsibility to oversee, supervise, and monitor the service provider's performance of covered activities. This requires the member to have in place specific policies and procedures that will monitor the service providers' compliance with the terms of any agreements and assess the service provider's continued fitness and ability to perform the covered activities being outsourced. Additionally, the member should ensure that NASD and all other applicable regulators have the same complete access to the service provider's work product for the member, as would be the case if the covered activities had been performed directly by the member.

Members should also include specific policies and procedures to determine whether any covered activities that the member is contemplating outsourcing are appropriate for outsourcing. To determine the appropriateness of outsourcing a particular activity, firms may want to consider certain factors, such as the financial, reputational, and operational impact on the member firm if the third-party service provider fails to perform; the potential impact of outsourcing on the member's provision of adequate services to its customers; and the impact of outsourcing the activity on the ability and capacity of the member to conform with regulatory requirements and changes in requirements.[5] These factors, however, are not meant to illustrate all of the factors a member may want to consider and are not meant to be an exclusive or exhaustive list of factors a member may need to consider.

In addition, members are reminded that outsourcing covered activities in no way diminishes a member's responsibility for either its performance or its full compliance with all applicable federal securities laws and regulations, and NASD and MSRB rules.

II. Activities and Functions that are Prohibited from being Outsourced

A. Activities and Functions Requiring Registration and Qualification

It is NASD's view that the performance of covered activities, which require qualification and registration, cannot be deemed to have been outsourced because the person performing the activity is an associated person of the member irrespective of whether such person is registered with the member. An exception would be where a third-party service provider is separately registered as a broker-dealer and the contracted arrangement between the member and the service provider is contemplated by NASD rules, MSRB rules, or applicable federal securities laws or regulations.[6] An example of such an exception would be a clearing agreement executed pursuant to NASD Rule 3230 between a member and a clearing broker-dealer.[7]

B. Supervisory and Compliance Activities

NASD has noted in previous guidance that the ultimate responsibility for supervision lies with the member.[8] Accordingly, a member may never contract its supervisory and compliance activities away from its direct control. This prohibition, however, does not preclude a member from outsourcing certain activities that support the performance of its supervisory and compliance responsibilities. For example, a member may implement a supervisory system designed by another party, which could include a computer software program that detects excessive trading in customer accounts. However, if a member chooses to implement such a system, it must make its own determination that the system implemented is current and reasonably designed to achieve compliance as required under Rule 3010. This may include, for example, monitoring the system to ensure that it functions as designed and that such design is of an adequate nature and breadth.[9]

Endnotes

1 A February 2005 joint report by the Joint Forum of the Basel Committee on Banking Supervision found similar trends in the use of outsourcing by financial firms. *See Outsourcing in Financial Services*, The Joint Forum of the Basel Committee on Banking Supervision (February 2005). The Joint Forum was established in 1996 under the aegis of the Basel Committee on Banking Supervision (Basel Committee), the International Organization of Securities Commissions (IOSCO), and the International Association of Insurance Supervisors (IAIS) to address issues common to the banking, securities, and insurance sectors, including the regulation of financial conglomerates. The Joint Forum is composed of an equal number of senior bank, insurance, and securities supervisors representing each supervisory constituency.

2 Examples of covered activities include, without limitation, order taking, handling of customer funds and securities, and supervisory responsibilities under Rules 3010 and 3012.

3 *See* Rule 3010(a) and (b); *Notice to Members (NTM) 99-45* (June 1999).

4 Rule 3012 also requires a member firm to have a written supervisory control system that will, among other things, test and verify that the member's supervisory policies and procedures are reasonably designed to achieve compliance with the applicable securities laws and regulations and NASD rules. Members are reminded that this requirement includes the testing and verification of their supervisory procedures regarding their outsourcing practices, including testing and verifying that any due diligence procedures meet the "reasonably designed to achieve compliance" standard. *See NTM 99-45* (June 1999) (providing guidance on the meaning of the term "reasonably designed to achieve compliance"). Such testing and verifying will help firms to ensure that their due diligence analyses of third-party service providers remain current and relevant.

5 Members may also want to consult a February 2005 IOSCO report for more factors that they should consider in connection with outsourcing. *See Principles of Outsourcing of Financial Services for Market Intermediaries*, IOSCO Technical Committee (February 2005). Another resource members may want to consider is the previously mentioned report by the Joint Forum of the Basel Committee on Banking Supervision. *Outsourcing in Financial Services, supra* note 1.

6 NASD does not view a third-party vendor as an associated person of the member if it solely provides services such as a trade execution and reporting system or automated data services in connection with back-office functions that, in turn, are utilized by registered or other associated persons of the member.

7 *See* Rule 3230(a)(1). Some members also enter into secondary or sub-clearing (sometimes referred to as "piggyback clearing") arrangements for clearing services with an intermediary firm that has an existing contract with a clearing firm instead of contracting directly with the clearing firm. Because intermediary firms do not always identify to clearing firms which accounts belong to the piggybacking firms, NASD has filed with the SEC a proposed rule change to Rule 3230 and Rule 3150 (Reporting Requirements for Clearing Firms) that would require intermediary firms to identify the accounts belonging to the piggybacking firms and that would require clearing firms to distinguish the data belonging to intermediary firms from the data belonging to the piggybacking firms.

8 *See NTM 99-45* (June 1999).

9 *See id.*