Updates
September 09, 2021

FINRA, Federal Banking Agencies Issue Guidance on Third-Party Risk Management

Recent guidance from financial industry regulators reminds market participants to remain mindful of their business, compliance, and operational obligations when incorporating technology vendors as a fundamental part of their infrastructure. The Financial Industry Regulatory Authority (FINRA) recently published guidance (FINRA Notice) cautioning regulated firms to ensure that their compliance obligations are being met in the context of systems and procedures that have been outsourced to third-party entities. The FINRA Notice follows proposed guidance that was recently published by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) (together, Banking Agencies and such guidance, the Proposed Guidance) that also addressed potential risks associated with third-party relationships and the need for regulated firms to take steps to ensure third parties are meeting compliance expectations. The bottom line is that regulated firms would be well served to take a close look at their diligence and monitoring of third-party service providers to ensure that their providers are fulfilling the agreed-upon terms of service and contractual obligations. Developing an appropriate record of vendor management and oversight is also key to protecting firms in the event of a regulatory inquiry.

We recommend that regulated firms undertake substantive and thorough due diligence when selecting third-party technology service providers. Not all providers are equal with regard to business, operational, and compliance tool offerings. Further, some regulated firms are required to have third-party service providers attest to certain and specific undertakings. If the third-party technology provider is unaware of financial service regulatory requirements, regulated entities should factor that into their decision-making. Regulated financial firms must have contractual terms combined with policies, procedures, and controls to monitor and surveil the third-party service providers' performance and adherence to the agreement(s). Further, these agreements cannot be static, but evolving as facts, circumstances, and technology evolves. Finally, regulated entities should, at a minimum, have biannual meetings with their service providers as a part of monitoring and updating processes and procedures.

Below are key takeaways for regulated firms and market participants followed by a more detailed summary of the recent guidance.

Key Takeaways

- Failure to take appropriate measures to ensure that third-party vendors meet compliance standards has consequences for regulated firms. The FINRA Notice recounts disciplinary actions taken against registered firms related to deficiencies caused wholly or in part by the firms' outsourcing to a third-party vendor. The U.S. Securities and Exchange Commission (SEC) has also announced enforcement cases related to similar failures to comply with securities laws.[1]
- Both the FINRA Notice and the Proposed Guidance reflect principles that have been articulated in previous regulatory statements or staff guidance; accordingly, they are unlikely to create significant new

compliance obligations for supervised firms. That said, for banking organizations in particular, adoption of the Proposed Guidance would streamline and clarify existing expectations and create a uniform supervisory standard.
- Neither the FINRA Notice nor the Proposed Guidance carry the force of law. But—coupled with the related enforcement actions—they both highlight regulators' continued focus on third-party risk management (TPRM) practices and underscore the importance of devoting resources and attention to compliance in this area. Regulated firms and market participants should carefully consider whether current and future third-party arrangements align with these expectations and seek outside expertise and counsel where appropriate.

Summary

Overview: Integration of Technology Improves Processes Yet Generates Concerns

Both sets of guidance by FINRA and the Banking Agencies below reflect the regulators' efforts to acknowledge the noted shift in the way that the capital markets and banking industries have embraced technology in core facets of operations. For example, in August, FINRA released a comprehensive report, Cloud Computing in the Securities Industry (FINRA Report), which details the integration of cloud-based services into traditional financial institutional models. With respect to broker-dealers specifically, the FINRA Report explains: "Cloud computing is transforming how broker-dealers operate by providing opportunities to enhance agility, efficiency, resiliency and security within firms' technology and business operations while potentially reducing costs. As a result, cloud computing is increasingly seen by many firms as an important architectural component to their infrastructure."[2] The FINRA Report states that "core cloud computing services" used by broker-dealers will include data storage, processing capacity, networking, and software applications. Additionally, there is an array of cloud services options that a broker-dealer may use in furtherance of its services, such as:

1. Infrastructure as a Service (IaaS), where the services are used by the broker-dealer but maintained by a third-party vendor who provides the services over the internet;
2. Platform as a Service (PaaS), where the broker-dealer has control over the applications that are being developed and deployed, but the services are layered on top of the IaaS service and, therefore, also maintained by a third-party vendor who provides the services over the internet; and
3. Software as a Service (SaaS), where the third-party vendor manages all the layers of software and hardware necessary to host, develop, and launch new applications and the broker-dealer "is effectively renting a full IT stack."[3]

While the FINRA Report has a particular focus on cloud computing services, it reflects a shift in approach, as market participants are increasingly outsourcing tasks such as data and records retention, communication, and cybersecurity to third-party vendors in order to make business processes more efficient. As noted in the FINRA Report—as well as in the guidance summarized below—outsourcing these core responsibilities is permissible but raises a number of significant risks for market participants in meeting regulatory obligations, including, without limitation, consumer protection, recordkeeping, and business continuity requirements.

FINRA Regulatory Notice 21-29

On August 13, 2021, FINRA published a notice reminding firms that their supervisory compliance obligations extend to relationships with third-party vendors (or sub-vendors). Regulatory Notice 21-29 (1) reiterates

applicable regulatory obligations; (2) summarizes recent trends in examination findings, observations, and disciplinary actions; and (3) provides questions that FINRA member firms may consider when evaluating their systems, procedures, and controls relating to third-party vendor management. The FINRA Notice supplements FINRA's 2005 Notice to Members, noting that since the 2005 notice, and "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 [v]endors to perform risk management functions and to assist in supervising sales and trading activity and customer communications."

A number of FINRA compliance obligations extend to third-party vendor relationships, such as FINRA Rule 3110, which requires member firms to establish and maintain supervisory systems designed to achieve compliance with applicable securities laws and regulations, and FINRA Rule 4370, which requires firms to maintain written business continuity plans and emergency contact information designed to enable member firms to meet their existing obligations during an emergency or significant business disruption. Additionally, FINRA expects its member firms to have reasonably designed cybersecurity programs and controls in place.

Of note, the FINRA Guidance highlights that FINRA staff has initiated and pursued enforcement actions against firms related to third-party vendor relationships that led to compliance deficiencies for the member firm. For example, FINRA disciplined member firms for failing to maintain adequate procedures and execute supervisory oversight to protect the confidentiality of their customers' nonpublic personal information in violation of FINRA Rules 3110 and 2010 and SEC Regulation S-P Rule 30 where a third-party vendor exposed customers' nonpublic personal information, either directly or as a result of insufficient anti-virus software and cybersecurity programs. Additionally, FINRA disciplined member firms for violating books and records and supervisory obligations rules due to vendor system malfunctions, vendors failing to provide non-rewriteable, non-erasable storage, or vendors failing to correctly configure default retention periods.

The FINRA Notice includes a number of questions for FINRA member firms to consider when evaluating whether their supervisory controls and policies and procedures appropriately address potential risks raised by third-party vendor relationships. FINRA urged firms to take a "risk-based approach" to vendor management that takes into account the sensitivity and complexity of the functions being outsourced. Finally, FINRA noted its awareness of the Proposed Guidance published by the Banking Agencies (as discussed below) and stated that it will monitor the guidance and consider comparable action, where appropriate.

Federal Banking Regulators' Interagency Guidance

On July 19, 2021, Banking Agencies invited comment on the Proposed Guidance for assessing and managing risks that arise from third-party relationships.[4] Managing such risks (i.e., TPRM) has been a key supervisory priority for each agency in recent years as banks increasingly have come to "rely on third parties for a range of products, services, and activities[, including] core bank processing, information technology services, accounting, compliance, human resources, and loan servicing."[5]

The Proposed Guidance would bring helpful and arguably overdue harmonization in an area that, to date, has been marked by overlapping and competing regulatory pronouncements that create compliance challenges for banking organizations subject to the supervisory jurisdiction of more than one agency. If adopted, the Proposed Guidance would replace the Federal Reserve's 2013 guidance, the FDIC's 2008 guidance, and the OCC's 2013 guidance and supplementary FAQs with a consistent framework banks can apply to satisfy federal regulatory expectations. It is based on the OCC's existing guidance, which many in the industry consider to be the most comprehensive—and also the most stringent—currently in effect. Because it would be issued as supervisory guidance, however, it will not carry the force of law.[6]

The Banking Agencies describe the Proposed Guidance as "a framework based on sound risk management principles" that should inform "all stages in the life cycle of third party relationships" and, importantly, takes into

"account the level of risk, complexity, and size of the banking organization and the nature of the third-party relationship."[7] It is meant to apply to the full range of third-party relationships a bank may enter—whether with true third parties (i.e., vendors) or corporate affiliates engaged to provide specific services.

The Proposed Guidance describes the third-party risk management life cycle and identifies principles and considerations that should inform each stage, including:

1. Developing a plan that outlines the banking organization's strategy, identifies the inherent risks of the activity with the third party, and details how the banking organization will identify, assess, select, and oversee the third party;
2. Performing proper due diligence in selecting a third party;
3. Negotiating written contracts that articulate the rights and responsibilities of all parties;
4. Allocating oversight, governance, and management of the relationship to, as applicable, the board of directors and executive management and providing for independent reviews of the third party's performance;
5. Conducting ongoing monitoring of the third party; and
6. Developing contingency plans for terminating the relationship in an effective manner.

Because it is risk-based, the Proposed Guidance explains that an institution's program for oversight and management of third-party relationships should be "commensurate with its size, complexity, and risk profile as well as with the level of risk and number of [its] third-party relationships."[8] Additionally, the Banking Agencies explain that "[n]ot all [third-party] relationships present the same level of risk to a banking organization" and, accordingly, that more "comprehensive and rigorous oversight and management" should be reserved for relationships supporting "critical activities" rather than lower-risk relationships.[9] For these purposes, a "critical activity" is one that could have a significant impact on the bank's operations, customer relationships, or finances if the third party failed to satisfy its obligations.[10]

The Banking Agencies have invited comment on the Proposed Guidance as well as 18 specific questions regarding its content and form. The comment period, which was initially set to conclude on September 17, 2021, has been extended by the Banking Agencies to October 18, 2021, due to commenters' requests for additional time to respond to the Proposed Guidance.

Endnotes

[1] *See* SEC, Press Release: SEC Announces Three Actions Charging Deficient Cybersecurity Procedures, (August 30, 2021); *see also* In the Matter of Cetera Advisor Networks LLC et. al., Release No. 92800 (August 30, 2021); In the Matter of Cambridge Investment Research Inc. and Cambridge Investment Research Advisors, Inc., Release No. 92806 (August 30, 2021); In the Matter of KMS Financial Services, Inc., Release No. 92807 (August 30, 2021).
[2] FINRA, *Cloud Computing in the Securities Industry*, (August 16, 2021), at *1.
[3] *Id.* at 4-5.
[4] 86 Fed. Reg. 38,182 (July 19, 2021). The Banking Agencies separately issued a companion document titled "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks" on August 27, 2021, providing targeted guidance on risks that may arise from business relationships with fintech companies. Although directed primarily at smaller institutions, the agencies make clear that "the content may be useful for banks of any size."
[5] 86 Fed. Reg. at 38,184.
[6] To this end, the Banking Agencies took care to note that the Proposed Guidance would be issued in accordance with the rule each agency recently adopted on the appropriate use of supervisory guidance. e.g., 12 CFR part 4, Appendix A to Subpart F (OCC); 12 CFR part 262, Appendix A (FRB); 12 CFR part 302, Appendix

A (FDIC).
[7] 86 Fed. Reg. at 38,182.
[8] 86 Fed. Reg. at 38,187.
[9] *Id.*
[10] *Id.*

Authors

Jamie A. Schafer

Partner
JSchafer@perkinscoie.com 202.661.5863

Logan S. Payne

Counsel
LPayne@perkinscoie.com 202.654.6265

Explore more in

Investment Management Financial Transactions Fintech

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

'Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers