Bond Case Briefs

Municipal Finance Law Since 1971

Novel Concerns in FINRA's 2019 Risk Monitoring and Examination Priorities Letter.

On January 22, 2019, FINRA released its 2019 Annual Risk Monitoring and Examination Priorities Letter (the "Priorities Letter"). Late last year, as part of FINRA360 – the organization's ongoing improvement initiative – FINRA announced its plans to consolidate its Examination and Risk Monitoring Programs, integrating three separate departments into a uniform program. As reflected in the title of the Priorities Letter, FINRA's priorities apply to both its examination program and its risk monitoring responsibilities.

In past years, FINRA's priorities consistently focused on areas such as suitability, outside business activities, private securities transactions, private placements, communications with the public, anti-money laundering ("AML"), best execution, fraud, market manipulation, net capital requirements, customer protection, trade and order reporting, recordkeeping, risk management, and supervision. This year, with respect to sales practice risks, FINRA emphasized that it will continue to review and monitor firms' customer suitability reviews, protection of senior investors, and controls relating to outside business activities and private securities transactions. FINRA will also continue to prioritize market and financial risk areas relating to best execution practices; manipulative trading activities; compliance with Exchange Act Rule 15c3-5 risk management controls; short sales and short tender activities; and credit risk and liquidity.

Notably this year, FINRA has highlighted five emerging areas of concern, which we focus on in this alert: (1) online distribution platforms; (2) supervision of digital assets business; (3) compliance with FinCEN's Customer Due Diligence Rule; (4) fixed-income mark-up and mark-down disclosure obligations; and (5) regulatory technology.

Online Distribution Platforms

The first highlighted item in the Priorities Letter pertains to securities offered through websites, which are described as "online distribution platforms." These types of securities offerings most commonly facilitate capital raising efforts under Rule 506(c) of Regulation D and Regulation A of the Securities Act of 1933. FINRA has observed that broker-dealers are increasingly involved in the distribution of securities through online platforms, raising concerns that firms are not complying with FINRA rules in the process. While FINRA has identified varying degrees of broker-dealer participation in such platforms – ranging from limited involvement of broker-dealers performing narrow functions such as custody, escrow, or back-office duties to full participation by broker-dealers that own and operate platforms – any firm participation in these activities will be subject to enhanced regulatory review. If a firm is associated with selling, recommending, or facilitating the sale of securities through an online platform, FINRA may evaluate how the firm:

- Conducts reasonable-basis and customer-specific suitability analyses for clients investing in online offerings. Depending upon the particular offering, a member firm may be required to demonstrate that it evaluated each investor's risk profile, tolerance, investment history, and goals.
- Ensures compliance with AML obligations. In accordance with the particular facts and

circumstances of each offering, a member firm should obtain appropriate information regarding the investors and sources of investment funds and determine how the transactions – both individually and in aggregate for the entire deal – will be reviewed.
- Evaluates the risks associated with offering documents and communications with the public. Given the widespread circulation of marketing materials targeting potential investors for participation in these offerings, a member firm should ensure that each offering meets FINRA's advertising regulation standards of being fair, balanced, and not misleading. This includes the disclosures contained in the offering materials, which may not include false or misleading statements, or omit material information.
- Addresses the risk of sales to non-accredited investors, specifically for offerings under Rule 506(c) of Regulation D. Given the variance in size, structure, and requirements of these offerings, guaranteeing participation by only "accredited" investors is essential. A firm should apply a risk-based approach when verifying that each investor qualifies as accredited (and thus allowed to participate in such offerings).
- Assesses the risk of excessive or undisclosed compensation arrangements between firms and issuers, specifically for offerings under Regulation A. A member firm should ensure that prospective investors have access to all the appropriate information regarding the offerings in which the firm participates, including where and how the funds are allocated.

Supervision of Digital Assets Business

Firms participating in activities related to digital assets are now a key priority for FINRA. The digital assets business encompasses cryptocurrencies, virtual coins, tokens, and any other use of distributed ledger or blockchain technology. In prior years, FINRA expressed concerns regarding the potential for harm to investors in the cryptocurrency and initial coin offering ("ICO") spaces. This year, FINRA has broadened its focus to the entire digital assets sector. As part of its efforts, on July 6, 2018, FINRA issued Regulatory Notice 18-20 which encouraged firms to notify FINRA if they plan to engage in activities related to digital assets. Firms are asked to notify FINRA of their involvement by July 31, 2019, during which time broker-dealers may find themselves subject to this year's examinations. In addition to complying with FINRA's request for information, member firms must ensure that their involvement in the digital assets business complies with FINRA Rules, including those regarding custody, sale, valuation, and AML.

Customer Due Diligence and Suspicious Activity Reviews

This year, FINRA will concentrate on assessing firms' compliance with the Financial Crimes Enforcement Network's ("FinCEN") final rule on Customer Due Diligence Requirements for Financial Institutions (the "CDD Rule"). The CDD Rule adds a "fifth pillar" to the Bank Secrecy Act ("BSA") and is intended to both clarify customer due diligence requirements for covered financial institutions[i] and strengthen their ability to detect, prevent, and report illicit activities. The CDD Rule codifies and expands upon existing BSA/AML requirements by explicitly requiring covered financial institutions to: (i) identify and verify the identities of the beneficial owners of legal entity customers; (ii) understand the nature and purpose of customer relationships in order to develop customer risk profiles; and (iii) conduct ongoing monitoring for suspicious transactions and, on a risk-basis, maintain and update customer information.[ii]

Previously, the BSA required covered financial institutions to develop written AML compliance programs that, at a minimum, consisted of the following four pillars: (i) a system of internal controls to ensure ongoing BSA/AML compliance; (ii) independent testing for compliance; (iii) a designated person or persons responsible for implementing and monitoring the operations and internal controls of the AML program; and (iv) ongoing training for appropriate persons. Consistent with these requirements, FINRA adopted Rule 3310 (formerly NASD Rule 3011) requiring all member firms to

maintain AML programs and procedures that satisfy the four pillars of the BSA, as well as put in place policies and procedures that can reasonably be expected to detect and cause the reporting of suspicious transactions. Because the CDD Rule requires firms to maintain appropriate risk-based procedures for conducting ongoing customer due diligence as a required "fifth pillar" for adequate AML compliance programs, FINRA is considering whether FINRA Rule 3310 should be amended to more closely align with FinCEN's CDD Rule.[iii]

FinCEN implemented the CDD Rule on May 11, 2016, and it became effective on July 11, 2016.[iv] Covered financial institutions had until May 11, 2018 to comply with the new provisions. Prior to May 11, 2018, under the BSA, covered financial institutions were required to create customer identification programs that included procedures to conduct due diligence on both individuals and legal entities opening new accounts. However, firms were not explicitly required to perform customer due diligence on the beneficial owners of legal entity customers. Now, incorporated into the fifth pillar of the BSA, the CDD Rule requires firms to maintain written AML procedures that are reasonably designed to identify and verify the identity of any individual who owns 25 percent or more of a legal entity customer, and at least one individual who controls the legal entity (i.e. the legal entity customer must identify its ultimate beneficial owner or owners and not "nominees" or "straw men.").[v]

With respect to the CDD Rule, FINRA indicated in its Priorities Letter that it will concentrate on the "data integrity [of a firm's] suspicious activity monitoring systems, as well as the decisions associated with changes to those systems." Because FinCEN allowed firms a lengthy two-year period to comply with the CDD Rule, most firms should already have in place systems that incorporate these new customer due diligence obligations. Nonetheless, some best practices for firms seeking to ensure compliance with the CDD Rule include the following:

- Confirm that all AML written supervisory policies and procedures are properly updated to incorporate CDD Rule obligations. The procedures should detail individual responsibilities in connection with the CDD Rule, including what party or parties will review and approve changes to a customer's risk profile. Procedures should also address instances in which the firm has obtained insufficient or inaccurate customer information.
- Conduct ongoing training for compliance professionals on new CDD requirements, including how to properly: (1) gather required customer information; (2) verify and record beneficial owners of legal entity customers; (3) conduct appropriate ongoing risk profiling; and (4) perform periodic customer reviews.
- Confirm that all internal and outsourced technologies used to perform ongoing customer due diligence are CDD Rule-compliant.
- Verify that customer due diligence reporting data is up-to-date and accurate.
- Confirm that customer risk profile information and collected beneficial ownership information is verified, recorded, and incorporated into AML compliance screening programs, and being used in connection with suspicious activity reporting.
- Check that current programs and procedures require the collection of beneficial ownership information for existing clients that open new accounts.
- Review all recordkeeping procedures for customer risk profiles, and beneficial ownership identification and verification information.
- Periodically conduct a sampling of new accounts opened and review customer data for compliance with the CDD Rule.

Fixed Income Mark-ups/Mark-downs on Trade Confirmations

Another focal point for FINRA's examination and risk monitoring programs this year will be firms' compliance with mark-up and mark-down disclosure obligations on fixed-income transactions with

customers, pursuant to last year's coordinated amendments to FINRA Rule 2232 (Customer Confirmations) and MSRB Rule G-15 (Confirmation, Clearance, Settlement and Other Uniform Practice Requirements with Respect to Transactions with Customers). Taken together, the amendments require member firms to provide retail customers with additional transaction-related information for certain trades in corporate, agency and municipal debt securities. Firms were previously required to disclose transaction cost information when acting as principal with customers for only equity trades, pursuant to Securities and Exchange Act Rule 10b-10. The amendments added comparable requirements for bond trades.

In its December 2018 Report on FINRA Examination Findings, FINRA noted certain critical failings in some member firms' implementation of changes required under FINRA Rule 2232 and MSRB Rule G-15 as amended. FINRA has included mark-up and mark-down disclosure obligations under revised Rule 2232 in the "Highlighted Items" section of its 2019 Priorities Letter. FINRA's repeated emphasis on firms' compliance with mark-up and mark-down disclosure obligations indicates that this is a significant area of concern that FINRA exam teams will scrutinize in the coming year.

FINRA Rule 2232 as amended requires member firms to disclose to retail customers the amount of mark-up or mark-down the customer paid for a purchase or sale in a corporate or agency debt security,[vi] if the member firm also executes one or more offsetting principal trades in the same security on the same trading day in an aggregate trading size meeting or exceeding the size of the trade with the customer.[vii] Mark-ups must be disclosed both as a total dollar amount for the transaction and as a percentage of the prevailing market price ("PMP") for the security – to be calculated pursuant to FINRA Rule 2121 (Fair Prices and Commissions). Rule 2232 also now requires customer confirmations to contain the time of execution of the trade and a security-specific link (with CUSIP) to the FINRA or MSRB website, where the customer can find additional details about the transaction.[viii]

For disclosure purposes, firms must "look through" to offsetting principal trades exercised by affiliate broker-dealers if those trades did not occur at arm's-length, and disclose the mark-up associated with those trades. While the amendments to FINRA Rule 2232 contain new disclosure obligations, there are two exceptions: i) member firms need not disclose mark-ups for principal trades executed on a functionally separate trading desk from the one that executes the customer trades (as long as the firm's policies and procedures are designed to ensure that the functionally separate trading desk has no knowledge of the customer trades); and ii) mark-up disclosure is not required for bonds that a member firm obtained in a fixed-price offering and subsequently sold to a retail customer at the same offering price on the same day.

Takeaways and potential pitfalls for member firms seeking to comply with FINRA Rule 2232 are as follows:

- FINRA Rule 2121 defines PMP presumptively as the contemporaneous cost incurred by the dealer when purchasing the debt security. When contemporaneous cost is not indicative of PMP, however, Rule 2121 sets forth nuanced waterfall provisions dictating the manner in which PMP must be calculated. Member firms using third-party vendors or automated systems to perform such waterfall analyses must have a reasonable basis to believe that the resulting PMP calculations are correct. The ultimate responsibility for calculating PMP and disclosing mark-ups in compliance with Rule 2232 lies with member firms.
- Individual brokers should receive adequate training and supervision to ensure that they understand what information to include in customer confirmations pursuant to Rule 2232, and the exceptions to the rule's disclosure requirements. Firms should also take reasonable steps to ensure that brokers do not intentionally delay execution of customer trades to avoid triggering Rule 2232's disclosure requirements.

- Member firms should consider periodically sampling and reviewing customer confirmations falling under Rule 2232's fixed income mark-up disclosure provisions to ensure that the information contained therein is complete and accurate.

Regulatory Technology

Like others in many industries, broker-dealers are turning to new and innovative technology to assist them in meeting their regulatory and compliance obligations. FINRA has identified Regulatory Technology as another highlighted area of focus in 2019. The Priorities Letter incorporates by reference a white paper FINRA published in September 2018 titled "Technology Based Innovations for Regulatory Compliance ("RegTech") in the Securities Industry," which contained a detailed discussion of common applications and implications for firms using RegTech to make compliance systems more efficient and effective. In doing so, FINRA identified five areas in which it observed member firms applying RegTech tools to conduct traditional compliance activities: (1) surveillance and monitoring; (2) customer identification and AML compliance; (3) regulatory intelligence; (4) reporting and risk management; and (5) investor risk assessment. FINRA noted that replacing traditional compliance functions with RegTech tools may present heightened risk to supervisory control systems, customer data privacy, and cybersecurity, among other areas.

Given the vast opportunities presented by RegTech, including improved surveillance quality and reduced costs, how are firms to decide which technologies to adopt and how aggressively to embrace these innovations? What are the known pitfalls to be avoided? What additional considerations should firms and compliance officers weigh? We provide the following four suggested tips to minimize regulatory exposure when implementing RegTech tools:

- **Maintain an Integration Plan**

Firms that see the long-term benefits of employing RegTech tools to automate compliance systems need to develop a risk-based integration plan. In the short-term, this likely means duplicating certain compliance efforts. Leaving old systems in place and comparing traditional data with results achieved through automated systems will permit firms to understand both benefits and shortcomings of new technology. In addition, to the extent tools engage in so-called "machine learning" to refine processes and increase output quality, those systems should be given a long enough learning curve to analyze what data falls away as false positives or noise. Firms should also conduct ongoing and rigorous testing of automated compliance systems to ensure efficacy.

Firms should also appreciate the disconnect between what FINRA calls structured and unstructured data when implementing RegTech tools. Marrying together data from disparate sources requires a well-planned long-term approach and may require keeping traditional compliance systems in place for years until a holistic RegTech system can be implemented and tested across all of a firm's business lines and information sources.

Though there have yet to be any RegTech-related enforcement actions taken by FINRA, a firm is more likely to avoid formal discipline if it takes a patient approach to implementation and makes several distinct efforts to identify blind spots before abandoning traditional compliance systems.

- **Envision the Worst-Case Scenario**

Firms should evaluate the impact automation has on their compliance systems under a worst-case scenario. When implementing new compliance systems, firms should determine the potential harm that would result from a system failure. For example, firms should ask whether the system impacts high regulatory priorities like protecting retail investors, achieving anti-money laundering

compliance or effecting regulatory reporting. Firms should also determine the scope of a potential system failure – is harm limited to a broken trade or failed wire transmission or would it have a widespread impact on market activity? Developing a risk matrix that accounts for these types of questions will enable firms to apply resources to the systems with the greatest potential for harm in areas of high regulatory priority.

- **Appreciate the Dangers of Outsourcing to Third-Parties**

Many of the early entrants in the RegTech tool development space are technology start-ups that offer products to financial institutions through third-party vendor support. This introduces risks concerning third-party data breaches and other data privacy concerns. FINRA has specifically cautioned that firms remain "ultimately responsible for compliance with all applicable securities laws and regulations and FINRA rules" in connection with outsourced activities or functions.

Step one for minimizing risks related to third-party vendors is to conduct reasonable initial and ongoing vendor due-diligence. Firms should ensure that vendors are technically, operationally and financially sound, and have adequate cybersecurity systems in place to safeguard data. Further, firms should be satisfied that they can adequately supervise the outsourced functions and that vendors understand regulatory requirements for record retention.

Firms must also be vigilant in protecting customer data. Whenever possible, firms should limit data provided to vendors to the minimum information essential to achieve the outsourced activity. For example, if a vendor conducts transaction review that is not related to customer identity, firms should ensure that the vendor cannot access customer-specific information. Firms should also ensure that customers provide consent as needed when new or additional information is collected by or shared with a third-party vendor.

- **Don't Be Afraid to Maintain a Dialogue with FINRA and Other Regulators**

FINRA has expressed a strong desire to foster an open dialogue with its members to help work through growing pains of emerging technologies. Consistent with this approach, FINRA has previously invited member firms and other interested parties to submit comments to identify benefits and risks associated with new financial technologies. FINRA consistently encourages stakeholders to actively engage with it on areas where additional guidance will support adoption of new technologies.

Member firms should take advantage of FINRA's willingness to listen and engage in active dialogue concerning RegTech by, among other things, notifying their regulatory point of contact when considering upgrading traditional compliance systems with new technology tools. Cooperating with regulators to identify potential technology failings not only increases the likelihood of "getting it right" but also helps make the case against formal action if something goes wrong.

FINRA's Priorities Letter, taken together with other recent notices and publications by the regulator, puts member firms on notice of the need to review and revise as appropriate their FINRA compliance programs both in areas of longstanding concern and in emerging areas of risk that FINRA took care to underscore. Firms should expect an increased focus by FINRA in examinations and risk monitoring in the highlighted areas of concern.

[i] The term "covered financial institution" includes U.S. banks, registered brokers or dealers in securities, mutual funds, and future commission merchants and introducing brokers in commodities. See 31 CFR § 1010.605(e)(1).

[ii] See 31 CFR §§ 1023.210(b)(5)(i) and (ii).

[iii] See FINRA Regulatory Notice 17-40, November 21, 2017 (The CDD Rule does not change the requirements of FINRA Rule 3310, but instead "amends the minimum statutory requirements for member firms' AML programs by requiring such programs to include risk-based procedures for conducting ongoing customer due diligence.").

[iv] https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf

[v] 31 CFR § 1023.210.

[vi] The security must also be a TRACE-Eligible Security required to be reported to TRACE under FINRA Rule 6730.

[vii] Because customers purchase bonds from member firms more often than sell them to member firms, for ease of reference our discussion going forward will refer only to mark-ups.

[viii] Firms must also include in the customer confirmation a brief description of the information available on the relevant website.

King & Spalding

February 22, 2019