Annual Broker-Dealer Regulatory Review and Outlook (2017)

compliance risk concepts

turning risk into reward

www.compliance-risk.com

Annual Broker-Dealer Regulatory Review and Outlook (2017)

Now that 2017 has ended and 2018 is emerging on the regulatory horizon, we find ourselves in a position to look back on what has transpired over the course of the past year in an effort to anticipate what the New Year may bring for BrokerD Dealers. Here is our perspective on what the highlights were in 2017, as well as what will be at the center of regulatory development in 2018.

2017 Review

FINRA Initiatives

Fourth quarter 2017 saw the announcement of FINRA's plan to consolidate enforcement functions into a single unit. They also initiated new, retrospective reviews of rules in several areas to ensure that they continue protecting investors in an efficient manner. Additionally, FINRA established the Innovation Outreach Initiative to encourage an ongoing dialogue with the securities industry that hopes to assist the self-regulator in better understanding financial technology innovations and their impact on the industry. FINRA also rolled out FINRA360, an extensive self-evaluation and organizational improvement initiative designed to review operations and improve overall processes when interacting with those it regulates. Over the past year, FINRA launched a new Compliance Calendar to help firms to keep track of upcoming filing requirements and other significant deadlines and educational opportunities. In addition, they developed a Compliance Vendor Directory designed to help firms engage compliance-related vendors

Overall, 2017 saw significant developments from the regulator, aimed at increasing clarity and transparency, as well as improving communication and engaging in a constructive dialogue with member firms.

FINRA 2017 Exam Findings Report

In December 2017, FINRA released its first ever Annual Exam Findings Report. The 14- page document focuses on noteworthy observations from recent exams that FINRA found to be worth highlighting due to their impact on the industry. FINRA was careful to add that the report is not a complete account of issues noted at member firms over the course of the year, nor does it serve to create any new regulatory requirements or interpretations of current ones. FINRA notes in the report that, as the exam program plays a central role in their "mission of investor protection and market integrity," hopefully the annual summary of findings will aide member firms in enhancing or refocusing their compliance, supervisory, and risk programs. Summarized below are some of the highlights of FINRA's 2017 exam findings report.

I. **Cybersecurity**: The report notes that, as the "nature and sophistication of cybersecurity threats continue to evolve, even robust cybersecurity programs can be compromised when, for example, an employee opens an email attachment that contains malware." Common threats observed by FINRA in 2017 included phishing and ransomware attacks, as well as fraudulent third-party wires. Most often, the latter employs the use of stolen client credentials or hacked and/or spoofed email

credentials. FINRA observed that there were a variety of areas where firms could improve their programs against threats. The report notes that firms with effective cyber programs often had well established governance structures and processes that address cybersecurity from a risk management perspective. Additionally, FINRA calls out ongoing employee training, use of system behavior analytics, strict division of duties, and oversight of branch office network security as effective tactics for managing cybersecurity risk. FINRA cautions member firms to pay careful attention to the inherent risks associated with vendors, and recommends performing methodical review and due diligence for all new (and current) vendors with respect to cybersecurity and data loss prevention, particularly when client data is involved.

a. Our Take: Firms should consider "as needed" employee training (in addition to annual) to help keep employees abreast of rapidly evolving threats. The human element of the industry is most often the most vulnerable to cyber-attacks, and phishing and spear phishing attacks are becoming not only more prevalent, but continuously more innovative and complex. Firms may wish to consider engaging an outside firm or leveraging the firm's IT department to perform social engineering testing, i.e. sending mock phishing emails purporting to be clients or financial advisors, in an attempt to convince firm employees to release personally identifying information or funds. Reviewing the results of such testing can serve as a useful training tool. On the network side of things, ***CRC recommends engaging a third-party vendor to perform penetration testing on the firm's network to assess the functionality of security measures (firewalls, etc.) and identify areas needing improvement***. ***Performing a gap analysis of cyber and information security policies is also extremely helpful.*** Additionally, carrying out a periodic review of all systems, including cataloging all systems and devices utilized by the firm and performing a risk assessment for all systems, is a useful exercise for confirming where private information is held and identifying any risk areas that need to be addressed.

II. Product Suitability: FINRA concerns with respect to the suitability of certain products and their supervisions did not vary materially by firm size, but did occur most frequently in connection with unit investment trusts (UITs) and leverage and inverse exchange traded funds (ETFs). The report notes that firms that employed a variety of effective practices for appropriately recommending the purchase or sale of such products. They specifically note that employee training with respect to the risk of these products and well as establishing standardized criteria for determining whether products are suitable for specific clients are among the most effective ways of managing associated risks.

a. Our Take: Product and strategy recommendations must be based on the information obtained "through the reasonable diligence of the member or associated person to ascertain the customer's investment profile."(FINRA SUITABILITY RULE 2111) A client's investment profile includes details such as: age, other investments, financial situation and needs, tax status, investment objectives, investment experience, investment time horizon, liquidity needs, and risk tolerance. To that end, best practices that firms should consider include maintaining appropriate paperwork for all new clients (to be completed at account inception), multi-level review practices in place for this paperwork to ensure that all required information had been provided, and periodic employee training with respect to product suitability. Additionally, periodic confirmation of information collected from clients is ideal, so as to ensure that information is accurate and no material changes to a client's circumstances affect the suitability of strategies and products being recommended.

III. **Anti-Money Laundering Compliance:** FINRA noted instances where firms "failed to establish and implement an AML program reasonably designed to detect and cause the reporting of suspicious activity." FINRA observed that firms with effective AML programs actively "tailor their risk-based AML program to the firm's business model and associated AML risks as opposed to simply implementing a more 'generic' program." These firms also conducted independent testing, which included sampling customer accounts to test whether the firm was collecting and verifying customer identification information, as well as trading and money movement activity to test whether the firm was performing adequate monitoring and investigation of suspicious activity. Effective programs "designed training programs that were specific to the roles and responsibilities of participating employees and evolving aspects of the AML landscape."

a. **Our Take:** Firms should contemplate enhancing annual training for all staff reviewing for questionable activity to confirm that they understand firm policies, are able to identify red flags, and know when and how to appropriately escalate potentially suspicious activity. Additionally, firms may wish to consider having "as needed" training in the wake of new newly identified threats. As part of their ***required annual independent testing of their AML program***, firms should evaluate current review processes to ensure that all risk areas are covered, for example, confirming that operational and suspense accounts are not excluded from data being reviewed, as foreign currency may pass through these accounts. Another tool firms may consider is performing an AML risk assessment to identify systems, processes, and other areas that pose or are exposed to the greatest risk in this area.

IV. **Best Execution:** FINRA defines best execution as a "significant investor protection requirement." FINRA noted in the report that it had concerns regarding the duty of best execution at firms of all sizes that receive, handle, route, or execute customer orders in equities, options, and fixed income securities. They found that "some firms failed to implement and conduct an adequate regular and rigorous review of the quality of the executions and their customers' orders." Firms that "established, maintained, and enforced policy and supervisory procedures regarding regular reviews for execution quality" and documented such reviews well were in the best position for proving best execution as well as identifying any instances in which best execution was not achieved.

a. **Our Take:** Firms may wish to consider implementing or enhancing an ***independent review of best execution***, performed outside of the trading department. Reviews should include all market and security types, and should compare the quality of the executions obtained via a firm's order routing and execution arrangements against the quality of the executions they could have obtained from competing markets. Such reviews should be well documented, and all exceptions should be uniformly escalated and resolved.

Looking Forward to 2018

FINRA Initiatives

In a letter from FINRA president Robert Cook, he noted that many priorities from last year remain at the top of their list this year with respect to both rulemaking initiatives and examinations. Additionally, FINRA's letter indicates a heightened sensitivity surrounding issues relating to senior investors.

FINRA expects to improve or augment measures to increase information sharing with firms during examinations, improve processes for making examination information requests, and enhance training of examiners. In addition, they are continuing other FINRA360 initiatives and have indicated that they will implement additional tools aimed at assisting firms in meeting compliance requirements.

Report Cards

In 2018, FINRA will launch several new report cards to assist firms with improving their compliance efforts:

- The Auto Execution Manipulation Report Card will highlight and assist firms with their supervision efforts to identify instances in which a market participant uses non-bona fide orders to move the NBBO.
- The Alternative Trading System Cross Manipulation Report Card will identify instances in which a market participant engages in potential manipulation of the NBBO, which results in the modification of a security's prevailing midpoint price on an alternative trading system crossing venue.
- The Fixed Income Mark-up Report Card will provide information to firms and the industry, which firms will be able to display based on certain criteria such as investment rating, product (e.g., corporate or agency) and length of time to maturity.

Exam Priorities 2018

FINRA recently published its annual Regulatory and Examination Priorities Letter. FINRA encourages broker-dealers to use the 2017 Annual Exam Findings Report and the 2018 Exam Priorities letter as resources to enhance their compliance, supervisory, and risk management programs, and to prepare for FINRA examinations. Outlined below are the key points from the letter.

I. **Technology Governance**: FINRA will review firms' information and technology change management policies and procedures. FINRA noted they have observed that some firms are at risk for or have experienced substantial customer service and regulatory issues as a result of operational interruptions caused by either the implementation of new systems or enhancements and modifications to existing proprietary or vendor systems. FINRA cautions that it is critical that firms maintain strong controls over changes to their information technology to prevent inaccurate, incomplete, untested or unauthorized changes to their production environments. These can result in system defects or outages, data inaccuracies or unintended consequences that can negatively affect customers, the firm, or the market.

   a. **Our Take**: Firms should have thorough, well documented Business Continuity Planning documents, and should train all employees with regard to these procedures. The BCP should reflect the firm's plans with respect to disaster recovery, backing up the network and systems, remaining operational without physical access to office locations, etc. Additionally, firms should take BCP practices under consideration when selecting vendors, and may additionally consider requesting BCP documents or writing BCP clauses into contracts. ***CRC recommends leveraging an outside firm to assist in creating BCP or performing a gap analysis of current BCP.***

II. **Cybersecurity:** Cybersecurity threats remain a significant risk and will continue to be a priority. The letter states that FINRA will evaluate the effectiveness of firms' cybersecurity programs to protect personally identifiable information from both external and internal threats. FINRA will review firms' preparedness, technical defenses, and plans for returning to normal operations, among other things. FINRA also reminds firms that they must have policies and procedures in place to assess whether to file a SAR when they identify a cybersecurity event.

a. **Our Take:** As noted above, the key best practices that firms should consider are focused around continual employee training to help keep employees abreast of constantly evolving threats, penetration testing, and performing a periodic review, risk assessment, and inventory of all systems to confirm where private information is held and identify any risk areas that need to be addressed. ***CRC performs penetration testing, gap analysis, and composition of policies and procedures.***

III. **Initial Coin Offerings and Cryptocurrencies:** Digital assets (such as cryptocurrencies) and initial coin offerings (ICOs) have received significant media, public and regulatory attention in the past year. FINRA plans to monitor the potential role firms and registered representatives could play in effecting transactions in such assets and ICOs. FINRA may review the mechanisms firms have put in place to ensure compliance with relevant federal securities laws and regulations and FINRA rules.

a. **Our Take**: ICOs involve new technologies and products that are highly technical and complex, and investors can lose some or all of the money they invest in an ICO. As such, it is important for member firms to determine whether an ICO constitutes a securities offering. If so, federal securities laws will apply. There are many questions that firms may wish to consider before pursuing or recommending and ICO to investors. For example, are the individuals or companies selling the investment registered financial professionals? Consider using FINRA's BrokerCheck tool to confirm. If they are not, this should be a red flag to potential investors. Additionally, inquire as to how can investors get their money back. Information provided to investors about ICOs should clearly describe this process. Ask the company if if tokens can be cashed in for a refund or sold within a secondary market. Consider what the company does. To date, most ICOs are being offered by startup businesses that have not rolled out a final product or platform to the market. This means that the information available at the time of an ICO may be incomplete, subject to change and difficult to verify. Lastly, be sure to inquire about steps companies have taken to protect their platforms and products from possible protocol breakdowns, hacking, malware, and fraud. Member firms should exercise extreme caution when experimenting with investment in ICOs and digital currencies, and should keep abreast of any guidance or risk alerts published by FINRA.

IV. **Securities Backed Lines of Credit:** According to the letter, as the use of SBLOCs has increased significantly over the past few years, FINRA will review firms' compliance with sales practice and operational obligations that apply to SBLOCs. FINRA will assess the adequacy of disclosures firms provide customers regarding the potential risks associated with SBLOCs. Separately, where the SBLOC lender is an affiliate of the member firm or other third party, the firm must establish controls to allocate the collateral securing the SBLOC and ensure that the SBLOC collateral is not dually pledged for any other extension of credit (e.g., a margin arrangement with the firm).

a. **Our Take:** When recommending or marketing SBLOCs to clients, member firms should take steps to ***ensure that their disclosures adequately address associated risks***, including the potential impact of a market downturn, the potential tax implications if pledged securities are liquidated, and the potential impact of an increase in interest rates. Additionally, clients should be made aware of all of the terms of the loan, including when and how interest is calculated, as well as when and how interest payments will be made. Additionally, employee training is a useful tool. Periodic training of those employees who are in a position to market or recommend SBLOCs that underscores the biggest potential risks and how to best relay these risks to clients. Informed employees yield informed clients.

V. **Regulation SHO:** FINRA will increase focus on evaluating firms' compliance with Rule 201 of Regulation SHO, which requires firms to develop policies and procedures to prevent the execution or display of a short sale order at a price that is equal to or less than the national best bid when a Short Sale Circuit Breaker (SSCB) is in effect for a National Market System (NMS) security. If a firm's Rule 201 policies and procedures include an automated, rules-based control to ensure compliance, FINRA expects the firm to develop a supervisory system to test that the control works properly and to conduct thorough supervisory reviews both before and regularly after it is operational. If a firm chooses to rely on an exemption to Rule 201, it must ensure that its activity or short sale transactions qualify for the exemption. For example, FINRA has observed that firms engaging in exchange-traded fund arbitrage activity are availing themselves of the Domestic Arbitrage Exemption detailed in Rule 201(d)(3), although SEC written guidance states that (1) the exemption does not apply to such activity and (2) a "bona fide market making" exemption to Rule 201 does not exist. Finally, firms that choose to execute a short sale in reliance on an exemption to Rule 201 must mark the order and report the trade as short exempt.

a. **Our Take:** FINRA noted in its 2017 Exam Report that there were various areas where member firms could improve their policies and procedures surrounding Reg SHO. Firms may wish to consider being less reliant on third-party provided data. FINRA noted that firms often struggled with recordkeeping and oversight standards due to the fact that they relied almost entirely on the assumption that vendors were accurately accounting for open sell orders (as required by FAQ 2.5 concerning Regulation SHO) and properly marked orders (in accordance with Rule 200(g) of Regulation SHO.) Further, firms should enhance internal oversight over these functions and developing testing programs to ensure that the automated controls are operating appropriately. ***CRC provides clients with gap analysis of firm's current SHO policies and procedures.***

This list is not exhaustive; other focus areas include sales practice risks, a continued interest in product suitability, protecting investors from fraud, high risk firms and brokers, business continuity planning, AML practices and procedures, protection of customer assets, accuracy of firms' financial data, and market integrity, including: best execution, manipulation across markets and products, and fixed income data integrity. For the full letter, click here.

New for 2018: FINRA Rules and Amendments

I. **Financial Exploitation of Specified Adults:** FINRA Rule 2165 will become effective February 5, 2018, and permits members to place temporary holds on disbursements of funds or securities

from the accounts of specified customers where there is a reasonable belief of financial exploitation of these customers.

II. **Amendments to FINRA Rule 4512 (Customer Account Information):** An amendment to FINRA Rule 4512 requires members to make reasonable efforts to obtain the name of and contact information for a trusted contact person for a non-institutional customer's account. The amendment will become effective February 5, 2018.

III. **The Financial Crimes Enforcement Network's (FinCEN) Customer Due Diligence Rule (CDD Rule):** Firms have until May 11, 2018, to comply with FinCEN's CDD Rule. FinCEN issued the CDD Rule to clarify and strengthen customer due diligence for covered financial institutions, including broker-dealers. In the CDD Rule, FinCEN identifies four components of customer due diligence: (1) customer identification and verification; (2) beneficial ownership identification and verification; (3) understanding the nature and purpose of customer relationships; and (4) ongoing monitoring for reporting suspicious transactions and, on a risk basis, maintaining and updating customer information.

IV. **Amendments to FINRA Rule 2232 (Customer Confirmations):** The amended FINRA Rule 2232 requires a member to disclose the amount of mark-up or mark-down it applies to trades with retail customers in corporate or agency debt securities if the member also executes offsetting principal trades in the same security on the same trading day. The amended rule also requires members to disclose two additional items on all retail customer confirmations for corporate and agency debt security trades: (1) a reference, and a hyperlink if the confirmation is electronic, to a web page hosted by FINRA that contains publicly available trading data for the specific security that was traded and (2) the execution time of the transaction, expressed to the second. These amendments are scheduled to become effective on May 14, 2018.

V. **Margin Requirements for Covered Agency Transactions (Amendments to FINRA Rule 4210):** FINRA's new margin requirements for Covered Agency Transactions are scheduled to become effective on June 25, 2018. Covered Agency Transactions include (1) To Be Announced (TBA) transactions, inclusive of adjustable rate mortgage (ARM) transactions; (2) Specified Pool Transactions; and (3) transactions in Collateralized Mortgage Obligations (CMOs), issued in conformity with a program of an agency or Government-Sponsored Enterprise (GSE), with forward settlement dates. Members are reminded that the risk limit determination requirements under the amendments to Rule 4210 became effective on December 15, 2016.

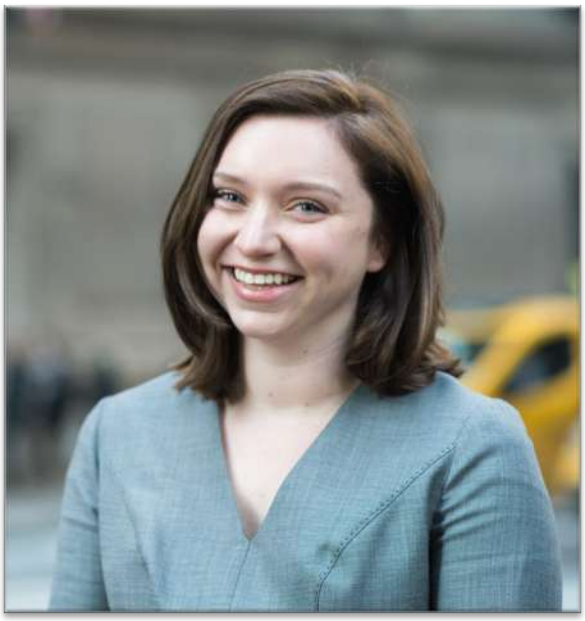
VI. **Consolidated FINRA Registration Rules:** The consolidated FINRA registration rules (FINRA Rules 1210 through 1240) will become effective October 1, 2018. The consolidated rules streamline, and bring consistency and uniformity to, the qualification and registration requirements.

Sources: FINRA 2017 Exam Findings Report, FINRA 2018 Exam Priorities Letter

Compliance Risk Concepts is a business-focused, team of senior compliance consultants and executives providing clients with the critical skills and expertise required to establish, maintain and enhance a balanced and effective compliance operational risk management program. With headquarters in New York, NY, and offices in Parsippany, NJ, Chicago, IL, and Westport, CT, CRC is your full-service Compliance Risk Management support partner. To learn more visit: http://compliance-risk.com/

CRC provides all services noted in bold. Feel free to contact Mitch Avnet at mavnet@compliance-risk.com with any questions or to schedule a call / meeting to further determine your individualized needs and requirements

ABOUT THE AUTHOR: ***KAITLYN GIBBS***



Kaitlyn Gibbs joined CRC in 2017. She is a regulatory compliance professional with 7 years of experience in the financial services industry. Kaitlyn has extensive knowledge of the rules of the Investment Company Act of 1940 and the Investment Advisers Act of 1940. She previously managed compliance processes and performed forensic testing in her role as Compliance Analyst at Welch & Forbes LLC.

She has experience performing annual reviews and risk analyses, regulatory research, as well as Code of Ethics administration. Her primary focus areas include, process implementation and enhancement, cybersecurity, marketing materials review, private equity investment compliance, and investment portfolio compliance.

Most recently at CRC, Kaitlyn has performed regulatory research, evaluated compliance programs, and performed annual reviews and risk assessments for investment advisors.

Kaitlyn holds a Bachelor's Degree in English from Boston University.

To learn more about Kaitlyn and the CRC leadership and team visit: http://compliance-risk.com/executive-leadership-and-team

www.compliance-risk.com

New York- Headquarters 441 Lexington Ave, New York, NY 10017 | 212.922.2844

New Jersey Office 300 Lanidex Plaza, Parsippany, NJ 07054 | 973.993.5557

Chicago Office 560 West Washington Blvd., Chicago, IL 60661 | 312-348-1348

Houston Office 12 Greenway Plaza, Houston, TX 77046 | 713-622-9939