

---

# 32<sup>nd</sup> Annual Meeting

---

## BROKER DEALER LIABILITY FOR 3<sup>RD</sup> PARTY SCAMS

Albert Copeland, Nicholas Guiliano,  
Catherine Mustico, Sander Ressler

<b>Broker-Dealer Liability for Third Party Scams, Nicholas J. Guiliano</b> .....	1
The Firm Imposter Scam.....	1
Broker-Dealer Liability Relating to the Transfer of Funds.....	2
Supervision of Transaction.....	2
Duties Arising Under Anti-Money Laundering Compliance .....	3
Customer Responses to AML Inquiries.....	5
Private Right of Action.....	5
AML Platforms and Procedures .....	6
Actimize .....	6
Discovery .....	6
<b>Anti-Money Laundering (AML)</b> .....	7
Bank Secrecy Act (31 U.S.C. 5311, <i>et seq</i> ) .....	10
Clearing v. Introducing Firm for AML.....	19
Past Disciplinary Actions.....	20
Discovery .....	21
Common Defenses .....	23
<b>Attachments:</b>	
Regulatory Notice 21-03, Fraud Prevention, February 10, 2021 .....	30
Regulatory Notice 21-36, Anti-Money Laundering and Countering the Financing of Terrorism, October 8, 2021 .....	40
Regulatory Notice 22-21, Heightened Threat of Fraud, October 6, 2022 .....	44
Regulatory Notice 20-13, Heightened Threat of Fraud and Scams, May 5, 2020 .....	49
Regulatory Notice 21-18, Cybersecurity, May 12, 2021 .....	57
FINRA Letter of Acceptance, Waiver and Consent, No. 2006004297301.....	69
FINRA Letter of Acceptance, Waiver and Consent, No. 2007009026302.....	77
BSA Timeline .....	88
FinCen Advisory, Advisory on Elder Financial Exploitation, June 15, 2022 .....	93
FINRA, Mary Schapiro Speech, March 22, 2004 .....	108
Risk Alert, Division of Examination, Observations From Broker-Dealer and Investment Adviser Compliance Examinations Related to Prevention of Identity Theft Under Regulation S-ID, December 5, 2022 .....	115
Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance, Kevin W. Goodman, June 18, 2015 .....	122
FINRA, 2021 Report on FINRA's Examination and Risk Monitoring Program, February 2021 .....	134
FINRA, Information Notice, Imposter Websites Impacting Member Firms, April 29, 2019 .....	180
Special NASD Notice to Members 02-21, Anti-Money Laundering, NASD Provides Guidance to Member Firms Concerning Anti-Money Laundering Compliance Programs Required by Federal Law .....	182
Regulatory Notice 09-64, Customer Assets, November 2009 .....	202
Regulatory Notice 12-05, Customer Account Protection, January 2012 .....	207

'Pig-Butchering' Scams a Top Investor Threat, According to State Regulators, Patrick Donachie, April 20, 2023. Wealth Management.com .....	211
Regulatory Notice 17-40, FinCEN's Customer Due Diligence Requirements for Financial Institutions and FINRA Rule 3310, November 21, 2017 .....	214
Regulatory Notice 19-18, Anti-Money Laundering (AML) Program, May 6, 2019 .....	222
Regulatory Notice 20-13, Heightened Threat of Fraud and Scams, May 5, 2020 .....	234
Regulatory Notice 20-30, Imposter Registered Representative Websites, August 20, 2020.....	242
Investor Alerts and Bulletins, Fraudsters Posing as Brokers or Investment Advisers – Investor Alert, July 27, 2021.....	248

**Public Investors Advocate Bar Association**  
**1300 McGee Dr., Ste. 112**  
**Norman, Oklahoma 73072**  
**Office: 405.360.8776**  
**E-Mail: [piaba@piaba.org](mailto:piaba@piaba.org)**

**2023 © PIABA**

*The information provided in this publication is for the convenience of the members of PIABA and is designed to provide practical and useful information on the subject matter being discussed. Although this information has been obtained from sources which we believe to be reliable, it does not constitute the rendering of legal advice and should not be used and/or otherwise relied on without independent verification. The information and opinions expressed herein do not necessarily reflect the views, policies and/or opinions of PIABA and/or its Board of Directors.*

## **Broker-Dealer Liability For Third Party Scams**

Third party scams exceed \$1 billion per year.

There are several types of scams. One scam includes the firm imposter scam.

### **The Firm Imposter Scam**

A customer is solicited to invest through a company, that sounds like a legitimate company, but instead is an imposter firm, with a very similar name. Customer wires money to often a foreign bank or the US correspondent of a foreign bank. The customer is given on-line credentials, and often a mobile application to track their investments, which of course quickly increase in value, inducing the investment of more funds.

When the customer tries to redeem their investment, the foreign entity, their web address, and their agents, suddenly disappear. In other instances, the customer is told that they can only redeem their funds if they pay local taxes, or some other fee. But, thereafter, the entire operation quickly disappears, and the accounts maintained by the fraudulent entity at the payee bank are also closed.

On May 5, 2020, FINRA warned its members of the continuing emergence of Firm Imposter Scams, whereby fraudsters obtain customer funds by impersonating legitimate securities broker-dealers or financial firms. FINRA Regulatory Notice 20-13 (May 5, 2020). On June 26, 2020, FINRA again warned “Be Alert For Impostors,” where again posing as legitimate firms imposter firms were using fictitious websites, and selling fictitious products, investors were lured into “wiring money to overseas third parties,” resulting in the investor potentially “losing hundreds of thousands of dollars to an imposter scam.”

The United States Securities & Exchange Commission also maintains a non-exhaustive list of Impersonators of Genuine Firms, and on July 21, 2021, issued an alert concerning “Fraudsters Posing as Brokers or Investment Advisers, whereby it also warned that “[f]raudsters may misappropriate the name, address, registration number, logo, photo, or website likeness” and using a number of tactics, including “Spoofed Websites,” trick investors into believing that they are conducting business with a legitimate securities firm.

The imposter scam is also known as the “Pig Butchering Scam,” *See, e.g.,* Donacti, P., Wealth Management, “*Pig-Butchering' Scams a Top Investor Threat*, According to State Regulators (April 20, 2023)(“Such schemes could also rebound on broker/dealers and advisors working with victims, particularly if money comes out of the victim’s brokerage account, according to Sander Ressler, director of Essential Edge Compliance Outsourcing Services”).

Since 2013, financial institutions have reported to the federal government over 180,000 suspicious activities targeting older adults, involving a total of more than \$6 billion. These reports indicate that financial exploitation of older adults by scammers, family members, caregivers, and others is widespread in the United States. Consumer Financial Protection Bureau, Office of Financial Protection for Older Americans, *Suspicious Activity Reports on*

*Elder Financial Exploitation: Issues and Trends* (Feb. 2019).

In 2017, the Consumer Financial Protection Bureau (“CFPB”) and the Financial Crimes Enforcement Network (“FinCEN”), issued a memorandum to financial institutions and law enforcement to combat elder financial exploitation, which highlighted the “critical role that financial institutions play in detecting, responding and preventing elder financial exploitation.” *Id.* at 3. According to the Report, “approximately 70 percent of filings were related to scams. Romance, relative in need, and lottery/sweepstake scams were the most common types of elder financial abuse described in these filings.”

### **Broker-Dealer Liability Relating to the Transfer of Funds**

Securities broker-dealers generally have limited responsibility for the transfer of funds which are duly authorized by the customer. Without more, securities broker-dealers may have no duty to investigate a customer’s intended payee.

However, Securities broker-dealers have a duty to supervise the transmittal of funds to third parties. Perhaps more importantly, under the “Customer Protection Rule,” SEC Rule 15c3-3, securities broker-dealers have a regulatory responsibility to safeguard and protect customer funds and securities from third parties. *See also*, Regulatory Notice 12-05, Customer Account Protection (January 2012).

### **Supervision of Transactions**

Rule 3012 regarding the establishment of a Supervisory Control System specifically requires all firms:

to establish, maintain and enforce written supervisory control policies and procedures that, among other things, include procedures that are reasonably designed to review and monitor the transmittal of funds (e.g., wires or checks) or securities:

- from customer accounts to third-party accounts (i.e., a transmittal that would result in a change of beneficial ownership);
- from customer accounts to outside entities (e.g., banks, investment companies);
- from customer accounts to locations other than a customer’s primary residence (e.g., post office box, “in care of” accounts, alternate address); and
- between customers and registered representatives (including the hand-delivery of checks).

NASD Rule 3012 (Supervisory Control System) and Incorporated NYSE Rule 401. *See also*,



Regulatory Notice 09-64 (Nov. 2009)(“FINRA firms must have and enforce policies and procedures governing the withdrawal or transmittal of funds or assets from customer accounts, including instructions from an investment adviser or other third party purporting to act on behalf of the customer”); FINRA Regulatory Notice 12-05 (Jan. 2012)(“firms must have adequate policies and procedures to review and monitor all disbursements it makes from customers’ accounts, including but not limited to third-party accounts, outside entities or an address other than the customer’s primary address”); *Department of Enforcement v. Ameriprise*, Letter of Acceptance Waiver & Consent, No. 2010-02515730 (March 1, 2013)(Ameriprise fined \$750,000 for Failing to Supervise and have reasonable supervisory systems in place to monitor wire transfer requests and the transmittal of customer funds to third-party accounts).

Rule 3012 also requires all member firms “to establish, maintain and enforce written supervisory control policies and procedures that, among other things, include procedures that are reasonably designed to review and monitor the transmittal of funds (e.g., wires or checks) or securities,” and cautioned members that the failure to do so, constituted a violation of FINRA Rule 3110, and the failure to supervise.

*See also*, Regulatory Notice 09-64 (Nov. 2009)(“FINRA firms must have and enforce policies and procedures governing the withdrawal or transmittal of funds or assets from customer accounts, including instructions from an investment adviser or other third party purporting to act on behalf of the customer”); FINRA Regulatory Notice 12-05 (Jan. 2012)(“firms must have adequate policies and procedures to review and monitor all disbursements it makes from customers’ accounts, including but not limited to third-party accounts, outside entities or an address other than the customer’s primary address”).

Securities broker-dealers are not relieved of their “Know Your Customer,” responsibilities simply because it is an “on-line” or “discount” broker-dealer.

Regardless of business model, a firm’s supervisory system must include written procedures for the review of customer accounts in compliance with the firm’s regulatory obligations. [E]xchange rules do not make a distinction between ‘discount’ firms and firms that conduct business on other than a discount basis.” Referring to Rule 405, the NYSE plainly stated that “[t]he Rule’s [405] requirements are imposed, including those routed via electronic trading systems.” A discount broker must “[s]upervise diligently all accounts handled by the organization.” NYSE Rule 405 (2). NYSE Information Memo 02-48 (November 7, 2002).

### **Duties Arising Under Anti-Money Laundering Compliance**

Title III of the USA PATRIOT Act, referred to as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Money Laundering Abatement Act), imposes obligations on broker/dealers. The Act requires firms to monitor for, detect and report suspicious activity conducted or attempted to the U.S. Treasury’s Financial Crimes Enforcement Network (“FinCEN”). 31 C.F.R. § 1023.320 (2021).

There is a direct connection between suspicious activity reports, third party fraud and elder exploitation. *Suspicious Activity Reports on Elder Financial Exploitation*, Consumer

Financial Protection Bureau (February 2019)(“Approximately 70 percent of MSB filings were related to scams. Romance, relative in need, and lottery/sweepstake scams were the most common types of scams described in these filings.”).

On March 5, 2017, FINRA also reminded its members that they “also must consider any obligations under FINRA Rule 3310 (Anti-Money Laundering Compliance Program) and the reporting of suspicious transactions required under 31 U.S.C. 5318(g) and the implementing regulations thereunder. (Regulatory Notice 11-17 at 3 n.11).

As stated above, in 2019, the CFPB and FinCEN issued a memorandum to financial institutions to combat elder financial exploitation highlighting “the critical role that financial institutions play in detecting, and responding, and preventing elder financial exploitation, as well as the important role of the filing of Suspicious Activity Reports (“SARs”) as part of these efforts. *See also*, Jason Foye, Director FINRA Anti-Money Laundering Investigative Unit and Brooke Hickman, Director FINRA Vulnerable Adults and Seniors Team, (“VAST”), *Overlapping Risks, Part 2, Anti-Money Laundering and Elder Exploitation*, November 10, 2020 (“SARs can and have been used to trigger investigations, support ongoing investigations and to identify previously unknown subjects and entities that are unfortunately targeting the vulnerable elder customers in the marketplace.”

With respect to Anti-Money Laundering, Notice to Members 02-21 requires that broker-dealers effecting transmittals or transfers of funds, including wire fund transfers, must collect, retain and record including the name and address of the transmitter and recipient, and “must verify the identity of transmitters and recipients that are not established customers.” (emphasis added). Notice to Members 02-21 also provides that “[b]roker-dealers also must establish internal controls to ensure that their AML policies and procedures are being enforced, including sufficient controls for the “monitoring for, detecting, and responding to “red flags.”

“Red flags” include, but are not limited, to circumstances “where the customer’s account has a large number of wire transfers to unrelated third parties inconsistent with the customer’s legitimate business purpose.” The Notice also suggests that “firms should also consider conducting computerized surveillance of account activity to detect suspicious transactions and activity [g]iven the global nature of online brokerage activity. *Id.* at 6.

Similarly on May 16, 2019, FINRA issued Regulatory Notice 19-18, reminding members of their obligations to monitor and report suspicious activity, providing a series of red flags that would alert firms to issues involving: (i) customer due diligence and interactions with customers; (ii) deposits in securities; (iii) red flags in securities trading; (iv) *red flags in money movement*; (v) red flags in insurance products; and (vi) various other potential red flags associated with the account or account activity. Regulatory Notice 19-18 (May 16, 2019)(emphasis added).

Regulatory Notice 19-18 also provides members a “non-exhaustive” list of “Potential Red Flags,” that broker-dealers are required to investigate in connection with “Money Movements” including, instances where:

- There is wire transfer activity that is unexplained, repetitive, unusually large,

shows unusual patterns or has no apparent business purpose.

- Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns.
- The customer makes high-value transactions not commensurate with the customer's known income or financial resources.
- The customer "structures" deposits, withdrawals below a certain amount to avoid reporting or recordkeeping requirements.
- There is an unusual use of trust funds in business transactions or other financial activity.

Regulatory Notice 19-18 at 7. (May 16, 2019). Regulatory Notice 19-18 also reminds members that "the failure to detect and investigate, and file suspicious activity reports with FinCEN constitutes a violation of FINRA Rules 3310 and 2010."

### **Customer Responses to AML Inquiries**

Customer represents that the purpose of the transfer is investment, (but the transfer is to an account not in the name of the customer).

Customer does not know recipient.

### **Private Right of Action**

There is no private right of action for the violation of AML Rules. However, the violation of these rules, and the duties associated with these rules, could support a finding of negligence. *See, e.g. Miley v. Oppenheimer & Co.*, 637 F.2d 318, 333 (5th Cir. 1981)(industry rules are "excellent tools against which to assess in part the reasonableness or excessiveness of a broker's handling of an investor's account"); *Lang v. H. Hentz & Co.*, 418 F. Supp. 1376, 1383-84 (N.D. Tex. 1976) (NASD Rules provide evidence of the standard of care a member should have); *Kirkland v. E.F. Hutton and Company, Inc.*, 564 F. Supp. 427 (E.D. Mich. 1983); *See also, Allen v. Lefkoff, Duncan, Grimes & Dermer P.C.*, 265 Ga. 374, 453 S.E.2d 719 (1995)(violation of Rule considered in determining negligence).

Again, securities broker-dealers may have no duty to investigate a customer's intended payee.

However, if a securities broker-dealer, via its AML responsibilities, obtains knowledge, or suspects that the customer or the payee may be engaging in fraud, or any other form of prohibited activity, the securities broker-dealer has a duty to investigate, and in certain instances, warn the customer. The failure to warn is a breach of fiduciary duty. *See, e.g., Twiss v. Kury*, 25 F.3d 1551 (C.A.11 (Fla.) 1994)(Under the common law, a person has no duty to control the conduct of another or to warn those placed in danger by such conduct *unless* a special relationship exists between the defendant and the persons whose behavior needs to be controlled

or the foreseeable victim of such conduct); *SII Investments, Inc. v. Jenks*, 370 F.Supp.2d 1213 (M.D. Fla., 2005)(duty to warn customers of adverse actions); *Glaziers and Glassworkers Union Local No. 252 Annuity Fund v. Newbridge Securities, Inc.*, 93 F.3d 1171 (3rd Cir. 1996)(Janney has a “fundamental” duty to warn, when “silence might be harmful.” *quoting, Globe Woolen Co. v. Utica Gas and Electric Co.*, 224 N.Y. 483, 121 N.E. 378, 380 (1918) (“A beneficiary, about to plunge into a ruinous course of dealing, may be betrayed by silence as well as by the spoken word.”)(Cardozo, J.).

## **AML Platforms and Procedures**

### **Section 314(b) of the USA PATRIOT Act**

FinCEN information sharing program

## **ACTIMIZE**

## **DISCOVERY**

Without revealing the existence of the filing of any Suspicious Activity Reports (“SARs”), all “non-confidential” documents, as defined by 31 CFR 103 (e)(1)(ii)(A)(2), upon which a SAR could be based, including, but not limited to, any business records, transactional documents, or account information, giving rise to the detection of suspicious conduct, or a pattern of suspicious conduct, with respect to Claimant’s account, or those payees, and payee banks, associated with wires or transfers made to or from Claimant’s securities accounts.

- Suspicious Activity Reports are protected from disclosure. However, documents, as defined by 31 CFR 103 (e)(1)(ii)(A)(2), upon which a SAR could be based, including, but not limited to, any business records, transactional documents, or account information are not protected from discovery.

It is well established that while the regulation prohibits disclosure of SAR’s and their contents, “courts have uniformly held that “supporting documentation” underlying a SAR that is generated or received in the ordinary course of a bank’s business is discoverable.” *Union Bank of California v. Superior Court of Alameda County*, 29 Cal. Rptr. 3d 894 (Cal. App. 3rd 2005); *quoting Whitney National Bank v. Karam*, 306 F.Supp.2d 678, 682 (S.D.Tex. 2004); *Gregory v. Bank One, Indiana, N.A.*, 200 F.Supp.2d 1000, 1002 (S.D.Ind. 2002); *United States v. Holihan*, 248 F.Supp.2d 179, 186 (W.D.N.Y. 2003); *See also, Cotton v. PrivateBank and Trust Co.*, 235 F. Supp. 2d 809 (N.D. Ill. 2002)(“this Court does not find the reasoning persuasive. Nothing in the Act or regulations prohibits the disclosure of the underlying factual documents which may cause a bank to submit a SAR.”); ,



# Anti-Money Laundering (AML)

# INTRODUCTIONS



Nicholas Guiliano



Catherine Mustico



Sander Ressler

# Anti-Money Laundering

AML refers to acts, laws, and regulations intended to stop criminals from disguising illegally obtained funds as legitimate income through money laundering.

Money Laundering describes the "washing" of dirty money:

The process by which illicit funds enter a legitimate financial system (Placement phase)

Obfuscate their origins through legitimate transactions (Layering phase)

Reintegrate as legal tender (integration phase)

# BANK SECRECY ACT (31 U.S.C. 5311, *et seq*)

The Bank Secrecy Act in the USA outlines the rules around AML procedures. Section 352 of the USA Patriot Act amended the Bank Secrecy Act to expand the organizations that need to implement due diligence procedures. Where previously only banks felt the full force of AML compliance, now non-bank financial institutions (such as broker-dealers) must also establish AML programs.

These businesses include (but aren't limited to):

Money service businesses

Real Estate Broker Services

Accountancy service providers

Broker-Dealers

Insurers

Estate agency services

Art market dealers

Bill payment services



# AT, THROUGH, or BY

- BSA requires financial institutions to assist the government to detect and prevent money laundering. Since 1970 the act has been amended to include other provisions and requirements to prevent the furtherance of ML at, through, or by financial institutions.
- Latest amendment to the BSA was on May 11, 2016 to include the Fifth Pillar of AML – The Customer Due Diligence Rule.
  - The amendments to FINRA Rule 3310 incorporate into the rule this **ongoing customer due diligence requirement** to conform the rule to the CDD Rule and aid member firms in complying with the CDD Rule's requirements.

# AML

BSA requires **ALL** financial institutions including broker-dealers to establish and implement AML programs.

Design to achieve compliance with the BSA **AND** *the regulation promulgated there under.*

- Must be designed to identify, monitor, and prevent ML. Must know essential facts about customer, also called CIP or KYC. (e.g customer's stated income is listed at \$25,000 - \$50,000/yr., but deposits/withdrawals through their account exceed \$300,000 - you need to ask the question...where is the money coming from?
  - Identify: red flags of suspicious activity
  - Monitoring: follow up on red flags – adequate investigation and follow through.



**POLICIES AND PROCEDURES:**

The BSA/AML program, including the internal controls prescribed therein, should be commensurate with the size and complexity of their institution's risk profile. The policy should be revisited and updated at least annually and be approved by executive management and/or Board of Directors.

**AML COMPLIANCE OFFICER:**

The AML Compliance Officer should be appointed by the Board of Directors and approved annually. He or she must be provided the tools and training to effectively manage the BSA program and also possess the expertise and authority sufficient to manage the BSA/AML Program.

**TRAINING:**

All staff must receive annual BSA/AML/OFAC training. The Board of Directors must also receive annual training. Materials used and attendance records must be documented. New employees should receive training prior to on-boarding. Training should be specific (ie, not just discussions of broad concepts) and tailored to the individual’s responsibilities tied to AML compliance.

**INDEPENDENT TESTING:**

Except in very limited circumstances, annual independent testing of their AML program is required. Testing must be done by internal staff or third parties independent from the processes. Results should be communicated to the Board/management in a timely manner. The implementation of recommendations and correction of findings should be tracked with periodic progress reports to the Board.

**CUSTOMER DUE DILIGENCE:**

Institutions must implement appropriate risk-based procedures for conducting ongoing customer due diligence. Understanding the nature and purpose of customer relationships, including business customers’ ownership structure and management control is critical. Ongoing monitoring of transactions and maintenance of up-to-date customer information is also required.





# AML Reporting/Due Diligence

Customer due diligence is a foundation of know your customer (KYC) processes and AML strategies. CDD requires companies to understand who their customers are, their financial behavior, and what kind of money laundering or terrorism financing risk they present.



## AML is not just for the purpose of filing SARs. It carries over to other areas of compliance and vice versa.

Andrew Ceresney, Director of Enforcement, Securities and Exchange Commission, stated "Regardless of the primary purpose of the due diligence or other data analysis that you or someone else in your firm are carrying out, information uncovered by these processes can be important information for multiple aspects of the compliance program. You must ensure that there is communication across different aspects of the compliance program and business, and ensure that siloes do not exist....The bottom line is that it is critical to ensure that AML compliance is integrated fully into the other compliance operations of the firm to ensure that suspicious activity detected by other compliance functions makes its way to the AML compliance function and vice versa."

"The SAR reporting obligations do not exist in a vacuum. Problems in BSA reporting often go hand in hand with problems elsewhere...."

"the information I have described above concerning the incidence of SAR reporting suggests there is a need to pursue standalone BSA violations to send a clear message to the industry about the need for compliance...."

Kevin W. Goodman, speech: Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance on 6/18/2015

“Detecting and reporting suspicious activity is a third fundamental aspect of AML compliance because, as set forth by Mr. Ceresney, the information you and your firms provide to regulators and law enforcement in SARs plays a vital role in helping regulators identify securities violations and bad actors in the markets. The SAR rule requires broker-dealers to report suspicious activity that involves or aggregates funds or other assets of at least \$5,000 and for which the broker-dealer knows, suspects, or has reason to suspect: 1) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any Federal law or regulation, 2) is designed to evade any requirement of the Bank Secrecy Act, 3) has no apparent business or lawful purpose or is not the sort of activity in which the particular customer would normally be expected to engage, or 4) involves the use of the firm to facilitate criminal activity. Once again I note that this goes far beyond traditional money laundering or terrorist financing. Under this rule, in identifying activity with “no apparent business or lawful purpose,” you should question trading activity that does not have a discernible investment or profit objective, companies with complex ownership structures that transfer money between accounts with unclear objectives, or the use of front companies to hide illicit sources of funds. Important red flags include the use of securities accounts for predominantly non-securities related types of transactions (e.g., wire transfers) and customers who seem to not care about high fees or losses in their accounts and appear more focused on the movement of funds. Broker-dealers with significant online access channels may want to take into account the source of login transmissions, particularly use of anonymous Internet nodes.”



“...AML includes far more than just preventing traditional money laundering...Broker-dealers must also monitor for and report suspicious activity, including activity that has no business or apparent lawful purpose. This goes beyond activity that implicates drug cartels or terrorist rings – it also includes activity that might indicate fraud, insider trading, or manipulative trading schemes.”

“...an AML compliance program can serve as a cornerstone of a firm’s overall compliance program...Your obligation is a proactive one, not a ministerial one... [The SEC takes] AML very seriously and will take great exception to firms that view AML as a peripheral or unimportant component of their compliance program.”

“...one particular area of focus will be the AML programs of clearing firms. OCIE believes that those institutions often have the “birds-eye view” of the market and are in the best position to identify patterns of activity engaged in by persons or entities that use more than one introducing broker...Examiners would expect clearing firms to use that high-level view of trading to monitor for suspicious patterns... **both the introducing firm and the clearing firm have responsibilities to detect and report suspicious activity that occurs by, at, or through their firm.**”

## The 5th Pillar FinCEN CDD Rule

- Ok, we get it. AML is more than just filing SARs and is about monitoring, escalating and investigating red flags. Anything else?

Firms must incorporate all aspects of BSA – including the CDD Rule. When the CDD Rule first came out, FINRA published NTM 18-19 explaining that, "On May 11, 2016, FinCEN, the bureau of the Department of the Treasury responsible for administering the Bank Secrecy Act<sup>2</sup> (BSA) and its implementing regulations, issued the CDD Rule to clarify and strengthen customer due diligence for covered financial institutions, including broker-dealers. In its 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.**"

As FINRA NTM 19-18 reiterated, "**Upon detection of red flags through monitoring**, firms should consider whether additional investigation, **customer due diligence measures** or a SAR filing may be warranted."



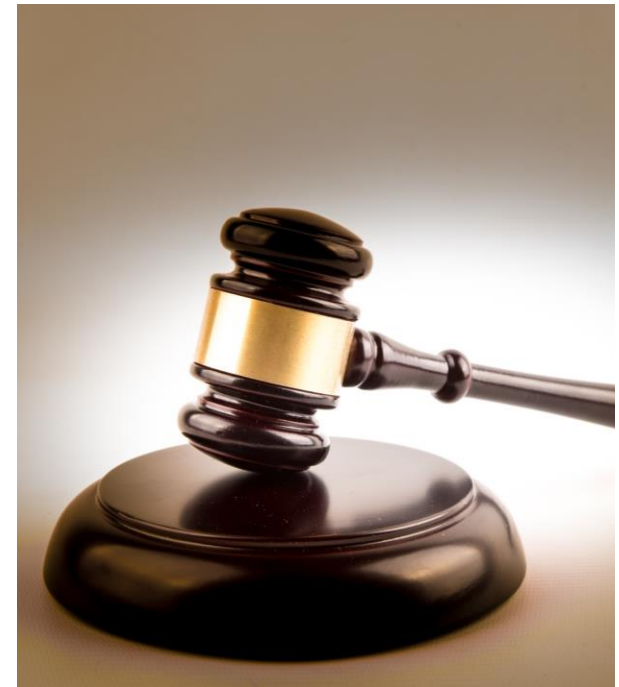
# Clearing v. Introducing Firm for AML

## Duties & Examples

- ✓ In FINRA's FAQ regarding Anti-Money Laundering publication, FINRA has answered the question 'Are all broker-dealers subject to the Bank Secrecy Act?' by stating, "Yes. The Bank Secrecy Act applies to all broker-dealers. There are no exemptions..."
- ✓ Additionally, in that same FAQ, FINRA has answered the question 'Can an introducing or clearing firm be relieved of AML obligations to the extent that the other is monitoring for suspicious activities?' by stating, "No. While a clearing firm can provide tools to help the introducing firm monitor its accounts for potential suspicious activity, all broker-dealers have an independent responsibility to comply with the suspicious activity reporting requirements. Introducing and clearing firms are both responsible for filing SARs for suspicious transactions "conducted or attempted by, at, or through" the firm."
- ✓ Remember, under the legal requirements, both the introducing firm and the clearing firm have responsibilities to detect and report suspicious activity that occurs by, at, or through their firm." – SEC Speeches
- ✓ "...one particular area of focus will be the AML programs of clearing firms. OCIE believes that those institutions often have the "birds-eye view" of the market and are in the best position to identify patterns of activity engaged in by persons or entities that use more than one introducing broker."

# Past Disciplinary Actions

- AWC 2006004297301 E\*trade Securities LLC and E\*Trade Clearing LLC. FINRA found both the clearing firm and the introducing broker-dealer separately and jointly responsible for conduct violation in the same matter. FINRA reiterated the firms AML obligations indicated that firms are expected to tailor their AML programs to their business and to the technological environment to which the firm operates. In this AWC FINRA stated that online firms such as E\*Trade have been instructed to “consider, conducting computerized surveillance of account activity to detect suspicious transactions and activity.”
- 2019061702701 Vision Financial Markets LLC and Vision Brokerage Services LLC. FINRA found both the clearing firm and the introducing broker-dealer separately and jointly responsible for conduct violation in the same matter. FINRA states firms had already been told they have a duty to look for red flags and a failure to tailor a firms AML procedures to its business and customer base and/or failure to monitor, analyze, and investigate red flags of suspicious activity constitutes a violation of FINRA rules 3310(a). In addition, a violation of any FINRA rule constitutes a separate and additional violation of FINRA rule 2010.



# DISCOVERY

## What to Request

- ✓ AMLCP
- ✓ WSP – specifically, their procedures for monitoring fund movements, escalation of Red Flags, and communication with the AML Department
- ✓ 3120 Annual Reports to Senior Management and 2 years of Independent AML test results
- ✓ Exception Reports (sometimes called Surveillance Alerts) and evidence of the Firm's response to them and a description of the parameters/thresholds
  - Note: You cannot ask for any SARs, as those are covered under SAR Confidentiality laws, but the underlying documents upon which a SAR is based is not. See the Federal Register Vol. 75, No 232
- ✓ KYC Documentation, Account Profiles, Call logs, and any internal notes on the account. Require them to identify the meaning of any internal classifications or common internal shorthand
- ✓ Risk Categories or level of monitoring

# DISCOVERY Vendor & Compliance

NTM 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."

# Common Defenses

- Customer Agreement, (indemnification, agreement that the clearing firm will have no duty to supervise or monitor the transactions
  - Cool story, bro. Firms cannot waive their obligations under Federal Law, including SRO Rules, vis-a-vis a contractual agreement where neither Uncle Sam nor FINRA was a party to that contact. There is nothing within FINRA Rule 3310, the BSA, or any implementing regulation promulgated thereunder that concludes with "unless the financial institution or broker dealer has an agreement with the customer that they will not meet this obligation."
  - Its also a violation of FINRA Rule 2268 and 2010 to attempt to waive liability. Specifically, in NTM 21-16, FINRA stated, "Accordingly, FINRA believes that it would be unethical and not in compliance with FINRA Rule 2010 for a member firm or associated person to attempt to seek indemnity from customers of costs or penalties resulting from the firm's or associated person's own violation of the securities laws or FINRA rules"
  - Those very same customer agreements also contain the duty of the Firm to transact business in accordance with the applicable regulations.
  - Additionally, if the Firm provides that defense, and provides evidence of that agreement, the Firm has demonstrated that the did not comply with FINRA's explicit instructions: "Member firms with customer agreements that include provisions that do not comply with FINRA rules should **take prompt steps** to ensure that their customer agreements fully comply with FINRA rules. Failing to comply with FINRA rules related to customer agreements may subject member firms to disciplinary action." In failing to do so, they violated FINRA Rule 2268, 2010, and 3110(a) for failing to supervise their compliance. OOPS.

# Defenses

- Failures under the BSA and 3310 only make them accountable to the government.

NTM 21-16 states, "For example, an indemnification and hold harmless provision that could be invoked to assert that a customer could not bring a claim alleging a failure to supervise against a member firm that the customer would otherwise be entitled to bring under applicable law would not comply with FINRA Rule 2268...In addition, a well-developed line of case law has held that it is contrary to public policy for a person to seek indemnity from a third party for that person's own violation of the federal securities laws."

- Footnote 17: See, e.g., *First Golden Bancorporation v. Weizmann*, 942 F.2d 726, 728-29(10th Cir.1991) (describing how "[c]ourts have rejected indemnity for a variety of securities violations because indemnity contravened the public policy enunciated by the federal securities laws")(citations omitted).
- Footnote 18: FINRA Rule 2010 requires a member, "in the conduct of its business," to adhere to "high standards of commercial honor and just and equitable principles of trade." The rule "states broad ethical principles and centers on the ethical implications of conduct[and] serves as an industry backstop for the representation, inherent in the relationship between a securities professional and a customer, that the customer will be dealt with fairly and in accordance with the standards of the profession." Steven Robert Tomlinson, Exchange Act Release No.73825,2014 SEC Lexis 4908, at \*17 & nn.17-19 (December11,2014) (citations omitted), *aff'd*, 637 F. App'x. 49 (2d Cir. 2016).

# Defenses

- The butler did it!
  - Blaming the vendor has no bearing on their responsibility to supervise, test, and monitor the activities of the Vendor in order to continue to have the reasonable reliance on that vendor
  - Blaming the customer for giving away access to their accounts, either by POA, or authorization has no impact on their independent duty to monitor transactions for red flags of suspicious activity.





# How to Work with Experts on AML

- Involve us early!
- Discovery Requests
- Many give assessments prior to engagement





# Q & A

A thin, light blue vertical line is positioned to the left of the text.

# BIOs

# Reference for Slides:

<https://haaslawpllc.com/2021/06/28/problems-with-our-anti-money-laundering-regulations/>  
PROBLEMS WITH OUR ANTI-MONEY LAUNDERING REGULATIONS

June 28, 2021 David Haas



MAY 9, 2022 | BRANDON ZERO

PE Adopts Quicker, Digitized Due Diligence to Cope with a Seller-Friendly Market

<https://www.themiddlemarket.com/news-analysis/pe-adopts-quicker-digitized-due-diligence-to-cope-with-a-seller-friendly-market>



<https://www.amlrightsource.com/news/improving-efficiency-and-your-financial-crimes-program>

Improving Efficiency and Your Financial Crimes Program

Picture of Elliot Berman Elliot Berman : June 08, 2023



Bank Secrecy Act & Anti-Money Laundering BSA/AML Testing, Validation and Consulting Services (Slide 7)

<chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.adiconsulting.com/wp-content/uploads/2022/08/AML-Pillars-2020.pdf>

<https://blog.flagright.com/key-components-of-an-aml-compliance-program>

Blog posts

Key Components of an AML Compliance Program

Admin

Sep 8, 2022



<https://www.freepik.com/free-photo/abstract-financial-freedom-still-life> arrangement\_18987452.htm#query=anti%20money%20laundering&position=4&from\_view=keyword&track=ais



# Regulatory Notice

21-03

## Fraud Prevention

### FINRA Urges Firms to Review Their Policies and Procedures Relating to Red Flags of Potential Securities Fraud Involving Low-Priced Securities

#### Summary

Low-priced securities<sup>1</sup> tend to be volatile and trade in low volumes. It may be difficult to find accurate information about them. There is a long history of bad actors exploiting these features to engage in fraudulent manipulations of low-priced securities. Frequently, these actors take advantage of trends and major events—such as the growth in cannabis-related businesses or the ongoing COVID-19 pandemic—to perpetrate the fraud.<sup>2</sup>

FINRA has observed potential misrepresentations about low-priced securities issuers' involvement with COVID-19 related products or services, such as vaccines, test kits, personal protective equipment and hand sanitizers. These misrepresentations appear to have been part of potential pump-and-dump or market manipulation schemes that target unsuspecting investors.<sup>3</sup> These COVID-19-related manipulations are the most recent manifestation of this type of fraud.

This *Notice* provides information that may help FINRA member firms that engage in low-priced securities business assess and, as appropriate, strengthen their controls to identify and mitigate their risk, and the risk to their customers, including specified adults and seniors,<sup>4</sup> of becoming involved in activities related to fraud involving low-priced securities. Firms that engage in low-priced securities business should also be aware of a recent SEC Staff Bulletin—[Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities](#)—that highlights for broker-dealers various risks arising from illicit activities associated with transactions in low-priced securities through omnibus accounts, particularly transactions effected on behalf of omnibus accounts maintained for foreign financial institutions.<sup>5</sup>

This *Notice* does not create any new requirements or expectations for member firms outside of their existing obligations pursuant to FINRA rules and applicable law, nor does implementing any of the practices cited here create a safe harbor from these obligations.

February 10, 2021

#### Notice Type

- Special Alert

#### Suggested Routing

- Anti-Money Laundering
- Compliance
- Financial Crimes
- Fraud
- Internal Audit
- Legal
- Operations
- Risk
- Senior Management

#### Key Topics

- Anti-Money Laundering
- Fraud
- Low-Priced Securities
- Trading

#### Referenced Rules & Notices

- Bank Secrecy Act
- FINRA Rule 2010
- FINRA Rule 2020
- FINRA Rule 2165
- FINRA Rule 3310
- FINRA Rule 6432
- Regulatory Notice 09-05
- Regulatory Notice 19-18
- Regulatory Notice 20-13
- Securities Act of 1933
- Securities Exchange Act of 1934

Questions regarding this *Notice* should be directed to:

- ▶ Greg Ruppert, Executive Vice President, National Cause and Financial Crimes Detection Programs, Member Supervision, at (415) 217-1120 or [greg.ruppert@finra.org](mailto:greg.ruppert@finra.org);
- ▶ Sam Draddy, Senior Vice President, Insider Trading, Fraud Surveillance and PIPEs Surveillance, Member Supervision, at (240) 386-5042 or [sam.draddy@finra.org](mailto:sam.draddy@finra.org); or
- ▶ Blake Snyder, Senior Director, Financial Intelligence Unit, Member Supervision, at (561) 443-8051 or [blake.snyder@finra.org](mailto:blake.snyder@finra.org).

## Background and Discussion

Broker-dealers play an important part in identifying and protecting investors from potentially fraudulent activity. A firm's failure to take appropriate steps as a gatekeeper to the public securities markets—for example, by not conducting a reasonable inquiry into a security's eligibility for distribution, where required—may expose that firm to liability risks, for example under Section 5 of the Securities Act of 1933 ("Securities Act").<sup>6</sup> In addition, Section 10(b) of the Exchange Act, Rule 10b-5 thereunder, and Section 17(a) of the Securities Act, as well as FINRA Rules [2010](#) (Standards of Commercial Honor and Principles of Trade), [2020](#) (Use of Manipulative, Deceptive or Other Fraudulent Devices) and [3110](#) (Supervision) establish obligations for member firms in connection with potential fraud. Firms also have obligations under the BSA and FINRA Rule [3310](#) (Anti-Money Laundering Compliance Program) to maintain appropriate risk-based procedures to conduct ongoing customer diligence and to report suspicious activity to the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury.

This *Notice* provides information to help firms strengthen their controls in four important areas related to potential fraud involving low-priced securities and thereby protect investors from financial harm and the firms themselves from financial, regulatory and reputational damage:

- ▶ **Detection:** the *Notice* describes possible red flags of potentially fraudulent low-priced securities activity;
- ▶ **Monitoring:** the *Notice* describes selected effective supervisory and other control practices FINRA has observed firms implement;
- ▶ **Suspicious Activity Report (SAR) filing:** the *Notice* describes firms' SARs filing obligations; and
- ▶ **Fraud Reporting:** the *Notice* describes additional avenues for firms to report potential fraud involving low-priced securities.

FINRA notes that a pattern of involvement in low-priced securities transactions—including soliciting customers, conducting offerings or executing transactions related to low-priced securities—informs FINRA's evaluation of a firm's risk profile. FINRA may examine or otherwise review more frequently the activity of firms that display these elevated risk characteristics.

### Detection: Potential Red Flags of Fraud Involving Low-Priced Securities

The red flags discussed below are intended to help inform firms about activity associated with potential fraud involving low-priced securities, including, but not limited to, schemes involving COVID-19 claims.<sup>7</sup> The red flags discussed in this *Notice* may overlap in some instances with red flags of suspicious anti-money laundering activity FINRA identified in [Regulatory Notice 19-18](#) (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations). This *Notice* provides firms engaged in low-priced securities business with more detailed information regarding red flags that are specific to potential fraud involving low-priced securities.

### Potential Indicators of Fraud Involving Low-Priced Securities

FINRA has observed that the following non-exhaustive list of issuer, third-party or customer activities may be red flags of fraud involving low-priced securities:

- ▶ Issuers
  - ▶ abrupt or frequent changes of issuer name, ticker symbol or business model, or abrupt expansion of an existing business model, often to benefit from the latest trend such as COVID-19 cures, test kits or prevention-related products (including instances in which the issuer has previously engaged in a business involved with other trends such as e-cigarettes, cannabis or cryptocurrency);
  - ▶ currently or previously a shell company;<sup>8</sup>
  - ▶ engaging in recapitalization or reorganization activities (*e.g.*, a reverse or forward stock split in conjunction with a reverse merger) that appear to concentrate the shares into the hands of a small number of shareholders, who may be acting in coordination;
  - ▶ hiring executive or control persons or service providers—such as attorneys, auditors, transfer agents, consultants and promoters—who have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers;
  - ▶ not providing current and adequate publicly available financial information<sup>9</sup> in SEC filings or voluntary disclosures on an inter-dealer quotation system;
  - ▶ making claims about projected scale and revenue targets that are not supported by the issuer's experience, assets or financial condition (*e.g.*, an issuer that develops cannabinoid-based products announces that it could earn millions in revenue from manufacturing and shipping COVID-19 home test kits);
  - ▶ making unsupported claims regarding partnerships, joint ventures or financing agreements with private entities (*e.g.*, an issuer promotes a press release touting the financial benefits of a new business partnership with a company whose financial condition cannot be independently verified);

- ▶ conducting increased social media, press release or related investor outreach campaigns after a period of apparent dormancy, particularly if the information is not confirmed on the issuer's website or in financial statements and disclosures filed with the SEC or on an inter-dealer quotation system, and often related to the latest trend; or
- ▶ lacking verifiable evidence of the issuer's business activities, such as limited or no operational website, social media accounts, references to issuer on employment websites or other independent reporting on the issuer's business activities.
- ▶ Third-Party Promotional Activities
  - ▶ hyping and promoting issuers (or their products or services), especially where the information cannot be reliably confirmed;
  - ▶ promotional investor email alerts, banner advertisements, dedicated promotional websites or seemingly independent news or research coverage, which prominently feature or advertise the issuer's new potential business prospects that (1) may be related to the latest trend (*e.g.*, winning a large contract or developing a new product or service), (2) may also present recent or projected investment returns, and (3) cannot be reliably confirmed;
  - ▶ generating a spike in social media promotions (*e.g.*, on Twitter, Instagram or Facebook), and activity on investor chat rooms or message boards; or
  - ▶ conducting unsolicited phone calls or sending text alerts to tout specific stocks to garner interest from registered representatives and investors.
- ▶ Firm Customers
  - ▶ customers that deposit large blocks of thinly traded low-priced securities, whether the securities are marked with a restrictive legend or not, particularly of issuers that recently changed business models to take advantage of the latest trend;
  - ▶ customers that engage in transactions that are consistent with an intent to affect the price of a low-priced stock, such as small purchases executed on behalf of a customer who owns a very large amount of the same low-priced stock, and do not have a legitimate investment rationale for the transactions;
  - ▶ customers that engage in a pattern of purchasing a low-priced security right before market close (which may be indicative of an attempt to mark the close);
  - ▶ customers or other parties that request the firm file a FINRA Form 211<sup>10</sup> to initiate or resume quotations for an issuer that recently changed business models—often to take advantage of the latest trend—or was recently subject to a trading suspension;
  - ▶ current officers, former officers, significant shareholders or family members of these individuals, who trade low-priced securities prior to a corporate announcement or stock promotion campaign;

- ▶ one or more customers suddenly trading the securities of a thinly traded issuer—often one that makes claims related to the latest trend—on opposite sides of the market, potentially leading to manipulative trading;
- ▶ customers, particularly specified adults<sup>11</sup>, who are being solicited to purchase low-priced securities where (1) the customer has not invested in low-priced securities previously; (2) the purchase is outside the customer's investment or risk profile; or (3) the low-priced security constitutes a large concentration of the customer's investments;
- ▶ multiple new customers opening accounts (particularly if they reside overseas and communicate with the firm only through electronic means) who either deposit shares of the same issuer or were introduced by the same individual to the firm; or
- ▶ customers, including financial institutions, that route high volume or frequent sell orders (with no buys) for low-priced securities to the firm for execution, including customers who maintain an execution-only relationship with the firm, or use omnibus or Delivery versus Payment/Receive versus Payment (DVP/RVP) accounts for such transactions.

### Monitoring: Supervisory and Other Controls

Measures that FINRA has observed firms implement in effective supervisory systems to mitigate risks associated with fraud involving low-priced securities include, but are not limited to, the following:

- ▶ Supervision of Associated Persons
  - ▶ monitoring registered representatives' customers' investments in low-priced securities that are marked "unsolicited" to determine if the trades were in fact solicited;
  - ▶ monitoring registered representatives' solicitations to customers to trade low-priced securities for compliance with FINRA rules and applicable laws;
  - ▶ monitoring the proprietary and customer accounts of registered representatives who primarily trade in low-priced securities; and
  - ▶ enhancing supervision of registered representatives who maintain direct or indirect outside business activities associated with companies with low-priced shares or trade in low-priced securities in their outside brokerage accounts.
- ▶ Account and Share Acceptance
  - ▶ establishing risk-based criteria to determine the characteristics of securities (e.g., exchange-listed and SEC reporting companies) investors may hold in their accounts or in which they may initiate transactions on the firm's platform;



- ▶ establishing controls to identify situations where customers open new accounts and deposit or transfer large blocks of low-priced securities, including in omnibus or DVP/RVP accounts;
  - ▶ promptly reviewing deposits of physical certificates and electronic transfers of low-priced securities prior to acceptance to identify low-priced securities that are marked as restricted, as well as low-priced securities that are not marked restricted where the restrictive legend may have been inappropriately lifted;
  - ▶ implementing risk-based acceptance policies regarding physical and electronic deposits of low-priced securities that incorporate factors such as whether the issuer is exchange-listed, the markets or exchanges on which it trades, any compliance flags that exchanges and over-the-counter markets provide regarding the issuer<sup>12</sup> and the existence of other red flags such as those referenced in this *Notice*;
  - ▶ requiring compliance or AML department approval of exceptions to firm policies on the deposit and trading of low-priced securities by customers; and
  - ▶ obtaining information regarding the customer's occupation or business and establishing risk-based criteria to request additional information, such as whether the customer is employed by a company that trades on the public markets and whether the customer intends to deposit or trade low-priced securities.
- ▶ Account Monitoring
- ▶ monitoring customer accounts for shifts in investment strategy away from listed equities towards unlisted low-priced securities, especially if this is inconsistent with the customer's stated or historic risk tolerance;
  - ▶ monitoring accounts held by specified adults and seniors for unusual purchases, or high concentrations, of low-priced securities and, where appropriate, contacting customers to determine if these decisions were the result of solicitation or influence by a third party;
  - ▶ monitoring customer accounts, including omnibus or DVP/RVP accounts, that are liquidating low-priced securities to address risks relating to the firm being engaged in, among other things, an unregistered securities offering;
  - ▶ establishing risk-based criteria to determine the circumstances under which a firm would consider placing restrictions on or closing an account;
  - ▶ monitoring for groups of related accounts trading in the same low-priced security at the same time; and
  - ▶ reviewing for indications of stock promotion activity in connection with share acceptance and account monitoring reviews.

► Other Controls

- conducting education and outreach—which could include providing risk alerts at the time of order entry—to customers, especially specified adults,<sup>13</sup> to inform them about the risks of investing in low-priced securities;<sup>14</sup>
- identifying and, if necessary, prohibiting customers from opening new accounts with, or depositing in existing accounts, restricted shares of low-priced listed or low-priced OTC securities; and
- increasing training and coordination between risk, compliance and operational personnel to ensure frontline staff are aware of red flags associated with potential fraud involving low-priced securities and schemes to unlawfully distribute unregistered securities and know how to report their concerns.

### Reporting Potential Fraud Involving Low-Priced Securities

FINRA Rule [3310\(f\)](#) and 31 CFR 1023.210(b)(5) require that member firms' AML programs include appropriate risk-based procedures for conducting ongoing customer due diligence, including procedures for conducting ongoing monitoring to identify and report suspicious transactions. In addition, FINRA Rule 3310(a) requires firms to "[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under [the BSA] and the implementing regulations thereunder;" the BSA and its implementing regulations require financial institutions to report suspicious transactions to FinCEN using SARs.<sup>15</sup> FinCEN has issued several notices and advisories noting emerging trends relating to illicit behavior connected to COVID-19, including investment scams and insider trading, and encouraged all financial institutions to enter the term "COVID19" or the specific term provided in a relevant FinCEN notice or advisory in Field 2 of the SAR and provide other requested information in the relevant fields and narrative.<sup>16</sup>

Financial institutions are also required to provide information to FinCEN in response to requests in furtherance of Section 314(a) of the USA PATRIOT Act for information regarding accounts reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering.<sup>17</sup>

Financial institutions subject to an anti-money laundering program requirement under FinCEN regulations, and any qualifying association of such financial institutions, are eligible to share information under Section 314(b) of the USA PATRIOT Act. Section 314(b) provides financial institutions with the ability to share information with one another, under a safe harbor provision that offers protections from civil liability, in order to better identify and report potential money laundering or terrorist financing. Although sharing information pursuant to Section 314(b) is voluntary, FinCEN and FINRA strongly encourage financial institutions to participate to enhance their compliance with anti-money laundering/counter-financing of terrorism requirements.<sup>18</sup>

Beyond the filing obligations discussed above, FINRA urges firms to protect customers and other firms by immediately reporting potential fraud involving low-priced securities to one or more of the following:

- ▶ FINRA's [Regulatory Tip Form](#) found on FINRA.org or through FINRA's [Whistleblower Tip Line](#) at (866) 96-FINRA;
- ▶ U.S. Securities and Exchange Commission's [system for tips, complaints and referrals](#) (TCRs) or by phone at (202) 551-4790;
- ▶ a local Federal Bureau of Investigation's (FBI) [field office](#); or
- ▶ local state securities regulators.<sup>19</sup>

In addition, firms should consider whether circumstances would trigger a reporting obligation pursuant to [FINRA Rule 4530](#) (Reporting Requirements).<sup>20</sup>

## Endnotes

1. For the purposes of this *Regulatory Notice*, the term “low-priced securities” refers to those securities that are sometimes referred to as “microcap stocks” or “penny stocks.” The term “microcap stock” generally refers to securities issued by companies with a market capitalization of less than \$250 to \$300 million. *See, e.g.*, U.S. Securities and Exchange Commission (SEC), [Microcap Stock: A Guide for Investors](#) (Sept. 18, 2013) and U.S. Securities and Exchange Commission, Investor Bulletin, [Microcap Stock Basics](#) (Sept. 30, 2016). The term “penny stock” generally refers to a security issued by a very small company that trades at less than \$5 per share. *See* [Fast Answers: Penny Stock Rules](#); Section 3(a)(51) of the Securities Exchange Act of 1934 (“Exchange Act”) and Rule 3a51-1 thereunder.
2. *See also* [Regulatory Notice 20-13](#) (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic).
3. As used here, “fraud involving low-priced securities” can include market manipulation and “pump and dump” schemes.
4. “Specified adult” as defined in FINRA Rule [2165](#) (Financial Exploitation of Specified Adults) refers to: (A) a natural person age 65 and older; or (B) a natural person age 18 and older who a firm reasonably believes has a mental or physical impairment that renders the individual unable to protect his or her own interests.
5. In addition to highlighting the risks described, the [SEC Staff Bulletin](#) also reminds brokers-dealers of their associated obligations under the Bank Secrecy Act (BSA), Rule 17a-8 under the Exchange Act, Section 5 of the Securities Act of 1933 (“Securities Act”), and FINRA rules. The Bulletin states that in the view of SEC staff, sufficiently discharging existing anti-money laundering (AML) obligations under the BSA requires broker-dealers to consider, among other things, the risks associated with the multiple layers of accounts through which transactions in low-priced securities may have been routed.
6. *See* [Regulatory Notice 09-05](#) (Unregistered Resales of Restricted Securities).
7. FinCEN has advised that as no single financial red flag indicator is necessarily indicative of illicit or suspicious activity, financial institutions should consider all surrounding facts and circumstances before determining if a transaction is suspicious or otherwise indicative of potentially fraudulent activities related to COVID-19. In line with a risk-based approach to compliance with the BSA, financial institutions also are encouraged to perform additional inquiries and investigations where appropriate. *See* [Advisory on Unemployment Insurance Fraud During the Coronavirus Disease 2019 \(COVID-19\) Pandemic](#).
8. *See* Exchange Act Rule 12b-2 (providing that a shell company is a “registrant . . . that has: (1) No or nominal operations; and (2) Either: (i) No or nominal assets; (ii) Assets consisting solely of cash and cash equivalents; or (iii) Assets consisting of any amount of cash and cash equivalents and nominal other assets.”).
9. *See* 17 CFR 230.144(c) (addressing “adequate current public information”).
10. *See* [FINRA Rule 6432](#) (Compliance with the Information Requirements of SEA Rule 15c2-11).
11. *See supra* note 4.

12. For example, the OTC Markets Group provides information on an issuer on the issuer's quote page and in the Group's Compliance Data feeds; these flags may identify an issuer as, for example, a shell company, bankrupt or delinquent in its SEC reporting.
13. *See supra* note 4.
14. Numerous resources are available at [https://www.sec.gov/oiea/investor-alerts-bulletins/ib\\_microcap\\_1.html](https://www.sec.gov/oiea/investor-alerts-bulletins/ib_microcap_1.html)
15. 31 U.S.C. 5318(g); 31 C.F.R. 1023.320. Under FinCEN's SAR rule, broker-dealers are required to file a SAR if: (1) a transaction is conducted or attempted to be conducted by, at, or through a broker-dealer; (2) the transaction involves or aggregates funds or other assets of at least \$5,000; and (3) the broker-dealer knows, suspects, or has reason to suspect that the transaction –
  - (a) involves funds or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law or regulation;
  - (b) is designed to evade requirements of the BSA;
  - (c) has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts; or
  - (d) involves the use of the broker-dealer to facilitate criminal activity.

31 C.F.R. 1023.320 (a)(2). The SEC maintains a SAR Alert Message Line at (202) 551-SARS (7277), which should only be used when firms have filed a SAR that requires the [immediate attention](#) of the SEC.
16. *See generally* [FinCEN's coronavirus webpage](#) and FinCEN's [March 20, 2020 guidance](#) discussing investment scams and insider trading. For types of suspicious activity related to specific types of conduct, FinCEN has requested more detailed keywords be included in Field 2 of the SAR form and other specific fields as well as the narrative. For general guidance on relevant BSA obligations, *see* [Notice Related to the Coronavirus Disease 2019 \(COVID-19\)](#).
17. 31 C.F.R. 101.520.
18. For updated guidance on the expanded acceptable use of the Section 314(b) information sharing authority, *see* FinCEN's December 10, 2020 [press release](#).
19. *See* NASAA's [webpage](#) providing contact information for state securities regulators.
20. For additional information about these requirements, *see* [Rule 4530 Frequently Asked Questions](#).

## Anti-Money Laundering and Countering the Financing of Terrorism

### FINRA Encourages Firms to Consider How to Incorporate the Government-wide Anti-Money Laundering and Countering the Financing of Terrorism Priorities Into Their AML Programs

#### Summary

The Financial Crimes Enforcement Network (FinCEN) has [issued](#) the first government-wide priorities for anti-money laundering and countering the financing of terrorism policy,<sup>1</sup> which was mandated by the Anti-Money Laundering Act of 2020 (AML Act).<sup>2</sup> FinCEN also issued a [statement](#) to provide covered non-bank financial institutions (NBFIs), including broker-dealers, with guidance on how to approach the AML/CFT Priorities.<sup>3</sup>

FINRA is issuing this *Notice* to inform member firms of the AML/CFT Priorities and the Statement, and to encourage member firms to consider how to incorporate the AML/CFT Priorities into their risk-based anti-money laundering (AML) compliance programs.

Questions concerning this *Notice* should be directed to:

- ▶ Victoria Crane, Vice President and Associate General Counsel, Office of General Counsel (OGC), at (202) 728-8104 or [Victoria.Crane@finra.org](mailto:Victoria.Crane@finra.org);
- ▶ Thomas Kimbrell, Associate General Counsel, OGC, at (202) 728-6926 or [Thomas.Kimbrell@finra.org](mailto:Thomas.Kimbrell@finra.org);
- ▶ Jason Foye, Senior Director, AML Investigative Unit, Member Supervision, at (561) 443-8062 or [Jason.Foye@finra.org](mailto:Jason.Foye@finra.org); or
- ▶ Nick Vitalo, Principal Counsel, OGC, at (646) 315-8474 or [Nicholas.Vitalo@finra.org](mailto:Nicholas.Vitalo@finra.org).

October 8, 2021

#### Notice Type

- ▶ Guidance

#### Suggested Routing

- ▶ Compliance
- ▶ Legal
- ▶ Operations
- ▶ Senior Management

#### Key Topics

- ▶ Anti-Money Laundering
- ▶ Compliance Programs

#### Referenced Rules & Notices

- ▶ Bank Secrecy Act
- ▶ FINRA Rule 3310
- ▶ Regulatory Notice 19-18
- ▶ Regulatory Notice 21-03

## Background and Discussion

### The AML/CFT Priorities

The AML Act became law on January 1, 2021, and, among other amendments to the Bank Secrecy Act (BSA), requires FinCEN to issue the AML/CFT Priorities and update them at least once every four years.<sup>4</sup> On June 30, 2021, FinCEN, the bureau of the Department of the Treasury responsible for administering the BSA and its implementing regulations, issued its first government-wide AML/CFT Priorities. The AML/CFT Priorities are intended to assist covered financial institutions,<sup>5</sup> including broker-dealers, in their efforts to meet their obligations under laws and regulations designed to combat money laundering and counter terrorist financing.<sup>6</sup>

The AML/CFT Priorities focus on threats to the U.S. financial system and national security and reflect longstanding and continuing AML/CFT concerns previously identified by FinCEN and other U.S. government departments and agencies.<sup>7</sup> They include predicate crimes to money laundering that generate illicit proceeds that illicit actors may launder through the financial system.<sup>8</sup> FinCEN set forth eight priorities: (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud (including securities and investment fraud and internet-enabled fraud); (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing. FinCEN provides details about each of the individual priorities and includes references to prior FinCEN advisories and guidance documents that identify related typologies and red flags that may help broker-dealers comply with their BSA obligations.<sup>9</sup>

### Incorporation of AML/CFT Priorities Into Firms' Risk-Based AML Compliance Programs

The BSA, as amended by the AML Act, provides that the “review by a financial institution” of the AML/CFT Priorities and “the incorporation of those priorities, as appropriate” into the risk-based AML compliance programs established by the financial institution “shall be included as a measure on which a financial institution is supervised and examined for compliance.”<sup>10</sup>

FinCEN has clarified that the publication of the AML/CFT Priorities does not create an immediate change in the BSA requirements or supervisory expectations for covered NBFIs, including broker-dealers.<sup>11</sup> FinCEN has noted further that covered NBFIs are not required to incorporate the AML/CFT Priorities into their risk-based AML programs until the effective date of final regulations promulgated by it.<sup>12</sup> The BSA, as amended by the AML Act, requires that FinCEN promulgate any appropriate regulations regarding the AML/CFT Priorities within 180 days of their establishment.<sup>13</sup>

FinCEN has stated that the final regulations will specify how financial institutions should incorporate the AML/CFT Priorities into their risk-based AML programs,<sup>14</sup> and that not every priority will be relevant to every covered institution.<sup>15</sup> FinCEN has also stated that covered NBFIs may nevertheless wish to start considering how they will incorporate the AML/CFT Priorities into their risk-based AML programs, such as by assessing the potential risks associated with the products and services they offer, the customers they serve, and the geographic areas in which they operate.<sup>16</sup>

FINRA Rule 3310 requires every member firm to develop and implement a written AML program reasonably designed to achieve and monitor for compliance with the requirements of the BSA and the implementing regulations promulgated thereunder by the Department of the Treasury. Although the issuance of the AML/CFT Priorities does not trigger an immediate change in the BSA requirements or supervisory expectations for member firms, FINRA encourages member firms to begin to evaluate how they will incorporate and document the AML/CFT Priorities, as appropriate, into their risk-based AML programs. Member firms that are beginning to evaluate how they will do so may wish to begin considering potential updates to the red flags that they have incorporated into their risk-based AML compliance programs in light of the risks presented by factors such as their business activities, size, the geographic locations in which they operate, the types of accounts they maintain, and the types of transactions in which they and their customers engage.

Firms may also wish to begin considering any potential technological changes that may be appropriate in order to incorporate the AML/CFT Priorities into their risk-based AML compliance programs, including changes to the technology that they use to monitor and investigate suspicious activity. Upon the effective date of final regulations addressing the AML/CFT Priorities, member firms should be in a position to review and incorporate, as appropriate, the AML/CFT Priorities into their risk-based AML programs.<sup>17</sup>

FinCEN has acknowledged the need for revised regulations and timely guidance to assist covered NBFIs, including broker-dealers, in complying with the BSA and expressed its commitment to working with federal agencies to develop and publish such guidance.<sup>18</sup>

Additional information about FinCEN's implementation of the AML Act is available on the dedicated [AML Act webpage](#) on FinCEN's website.



## Endnotes

1. [Anti-Money Laundering and Countering the Financing of Terrorism National Priorities](#) (AML/CFT Priorities) (June 30, 2021).
2. 31 U.S.C. § 5318(h)(4)(A) (as amended by AML Act § 6101(b)(2)(C)). The AML Act was enacted as Division F, §§ 6001-6511, of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (2021) (enacted) (enrolled bill available at <https://www.govinfo.gov/content/pkg/BILLS-116hr6395enr/pdf/BILLS-116hr6395enr.pdf>).
3. [Statement on the Issuance of the Anti-Money Laundering/Countering the Financing of Terrorism \(AML/CFT\) National Priorities](#) (Statement) (June 30, 2021). FinCEN also issued a joint statement with other regulators to provide guidance to banks on the AML/CFT Priorities. See [Interagency Statement on the Issuance of the AML/CFT Priorities](#) (June 30, 2021).
4. 31 U.S.C. § 5318(h)(4)(A) and (B) (as amended by AML Act § 6101(b)(2)(C)). FinCEN was required to consult with the Attorney General, Federal functional regulators (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)), relevant State financial regulators, and relevant national security agencies to establish the priorities and must continue to consult with these same parties when updating the AML/CFT Priorities. See *Id.*
5. Covered institutions are financial institutions required by BSA regulations to maintain an AML program. See 31 CFR §§ 1020.210(a) (banks); 1020.210(b) (banks without a Federal functional regulator); 1021.210 (casinos and card clubs); 1022.210 (money services businesses); 1023.210 (brokers or dealers in securities); 1024.210 (mutual funds); 1025.210 (insurance companies); 1026.210 (futures commission merchants and introducing brokers in commodities); 1027.210 (dealers in precious metals, precious stones, or jewels); 1028.210 (operators of credit card systems); 1029.210 (loan or finance companies); and 1030.210 (housing government sponsored enterprises).
6. AML/CFT Priorities, p. 1.
7. AML/CFT Priorities, pp. 2-3.
8. AML/CFT Priorities, p. 3.
9. AML/CFT Priorities. In [Regulatory Notice 19-18](#) (May 2019), FINRA provided a non-exhaustive list of red flags that may be applicable to the securities industry. In [Regulatory Notice 21-03](#) (February 2021), FINRA addressed additional red flags associated with potential fraud involving low-priced securities.
10. 31 U.S.C. § 5318(h)(4)(E) (as amended by AML Act § 6101(b)(2)(C)), 31 U.S.C. §§ 5321, 5324 and 5330(e) (2012); 12 U.S.C. §§ 1829b(j) and 1955 (2012).
11. Statement, p. 2.
12. Statement, p. 2. FinCEN also stated that until the effective date of final regulations, it will not examine covered NBFIs for the incorporation of the AML/CFT Priorities into their risk-based AML programs, and will not request that the staff of the U.S. Securities and Exchange Commission, Commodity Futures Trading Commission, Internal Revenue Service, or state financial regulators, or a self-regulatory organization (SRO) authorized to examine a covered NBFI, examine any covered NBFI for this requirement (or any related state requirement). *Id.*
13. 31 U.S.C. § 5318(h)(4)(D) (as amended by AML Act § 6101(b)(2)(C)).
14. AML/CFT Priorities, p. 2.
15. *Id.*
16. Statement, p. 2.
17. AML/CFT Priorities, p. 2.
18. Statement, p. 2.

# Regulatory Notice

## 22-21

## Heightened Threat of Fraud

### FINRA Alerts Firms to Recent Trend in Fraudulent Transfers of Accounts Through ACATS

#### Summary

FINRA alerts member firms to a rising trend in the fraudulent transfer of customer accounts through the Automated Customer Account Transfer Service (ACATS), an automated system administered by the National Securities Clearing Corporation (NSCC), that facilitates the transfer of customer account assets from one firm to another.

This *Notice* provides an overview of how bad actors effect fraudulent transfers of customer accounts using ACATS (referred to as ACATS fraud), lists several existing regulatory obligations that may apply in connection with ACATS fraud, and provides contact information for reporting the fraud. As FINRA continues to gather additional information related to ACATS fraud, FINRA is committed to providing guidance, updates and other information to help member firms stay informed about the latest developments, and will supplement this *Notice*, as appropriate.

Questions regarding this *Notice* should be directed to Jason Foye, Senior Director, Special Investigations Unit, at (561) 443-8062 or by email at [Jason.Foye@finra.org](mailto:Jason.Foye@finra.org).

#### Background & Discussion

NSCC Rule 50 established ACATS and sets forth the responsibilities of NSCC and the members that use ACATS. Among other things, the rule establishes the account transfer process and the attendant duties and obligations, and performance timeframes. Complementing ACATS is FINRA Rule [11870](#) (Customer Account Transfer Contracts), which governs the process by which customers can request a transfer of their securities account assets from one FINRA member firm to another and includes timeframes that align with those in NSCC Rule 50. In particular, FINRA Rule 11870 provides that within one business day of receiving the transfer instruction, the member firm carrying the customer's account (carrying member) must either validate (or accept) or take exception to (or reject) the Transfer Instruction Form (TIF) for reasons specified in the rule.<sup>1</sup> In addition, the rule states that the carrying member must complete the transfer within three business days following the validation of the TIF.<sup>2</sup>

October 6, 2022

#### Notice Type

- ▶ Special Alert

#### Suggested Routing

- ▶ Compliance
- ▶ Financial Crimes
- ▶ Fraud
- ▶ Internal Audit
- ▶ Legal
- ▶ Operations
- ▶ Risk
- ▶ Senior Management
- ▶ Trading

#### Key Topics

- ▶ ACATS
- ▶ Asset Transfers
- ▶ Fraud
- ▶ New Accounts

#### Referenced Rules & Notices

- ▶ Bank Secrecy Act
- ▶ FINRA Rule 2090
- ▶ FINRA Rule 3310
- ▶ FINRA Rule 4512
- ▶ FINRA Rule 4530
- ▶ FINRA Rule 11870
- ▶ NSCC Rule 50
- ▶ Regulatory Notice 20-13
- ▶ Regulatory Notice 20-32
- ▶ Regulatory Notice 21-14
- ▶ Regulatory Notice 21-18

In general, a customer who wishes to transfer securities account assets from the carrying member to another firm must open an account at the new firm that is expecting to receive the customer's account assets (receiving member). The account transfer process begins when the receiving member receives the customer's authorized TIF; the receiving member then initiates the account transfer through ACATS.<sup>3</sup> Typically, a TIF includes the customer's name, date, the account type and account numbers at the receiving member and carrying member, and other personal identifiable information about the customer (e.g., tax identification number or Social Security number).<sup>4</sup>

### Overview of ACATS Fraud

In a situation where customer account information is stolen, a bad actor may use this information to effect ACATS fraud. In general, ACATS fraud may unfold in the following manner:

Using the stolen identity of a legitimate customer of a carrying member, a bad actor will open a brokerage account online or through a mobile application in the name of the legitimate customer at the receiving member to create a new account. The bad actor may open the new account solely using stolen information or with a combination of stolen and false information (e.g., false email address or phone number).

Shortly after successfully opening the new account at the receiving member—generally, within a few days or weeks—the bad actor will then provide the receiving member with a TIF to initiate a transfer through ACATS of the legitimate customer's account assets from the carrying member.

Once the ACATS transfer of the assets to the newly established account at the receiving member is completed, the bad actor will (within a short period of time) attempt to move the ill-gotten assets to an external account at another financial institution by:

- ▶ transferring the account assets (*i.e.*, cash and securities) to an account at another financial institution;
- ▶ liquidating the securities or a portion of the securities transferred into the new account, then transferring any realized proceeds (along with any cash that was transferred to the new account) to an account at another financial institution; or
- ▶ purchasing additional securities using the transferred cash and then transferring those securities to an account at another financial institution.

ACATS fraud is related to the growing threat of new accounts being opened online or through mobile applications using stolen or synthetic identities.<sup>5</sup> In connection with the COVID-19 pandemic, FINRA previously advised member firms that bad actors may be “targeting firms offering online account opening services and perhaps especially, firms that recently started offering such services” by using stolen or synthetic identities to establish new accounts at member firms as a way to “divert congressional stimulus funds, unemployment payments or to engage in automated clearing house (ACH) fraud.”<sup>6</sup> Similarly, with ACATS fraud, bad actors may be taking advantage of the efficiencies of the account transfer process offered through ACATS to fraudulently transfer assets out of an existing account of a legitimate customer whose identity is stolen to a new account the bad actor established at another broker-dealer using the stolen identity.

### Relevant Regulatory Obligations

FINRA reminds its member firms of existing regulatory obligations that may apply in connection with ACATS fraud, including:

- ▶ FINRA Rules [2090](#) (Know Your Customer) and [4512](#) (Customer Account Information);
- ▶ the requirements of the Bank Secrecy Act and its implementing regulations and FINRA Rule [3310](#) (Anti-Money Laundering Compliance Program), including the requirements to maintain customer identification programs to verify the identity of each customer,<sup>7</sup> establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of Suspicious Activity Reports (SARs) with U.S. Treasury Department’s Financial Crimes Enforcement Network (FinCEN),<sup>8</sup> and to conduct ongoing customer due diligence, including monitoring to identify and report suspicious transactions;<sup>9</sup>
- ▶ the Identity Theft Red Flags Rule (Regulation S-ID); and
- ▶ the processing of customer account transfers through ACATS in compliance with FINRA Rule 11870 (Customer Account Transfer Contracts).

## Reporting Fraud

In addition to filing any required SARs through the [BSA E-Filing system](#), FINRA also encourages firms to immediately report potential fraud to:

- ▶ FINRA using the [Regulatory Tip Form](#) found on [FINRA.org](#);
- ▶ U.S. Securities and Exchange Commission's tips, complaints, and referral system (TCRs) or by phone at (202) 551-4790;
- ▶ the Federal Bureau of Investigation's tip line at 800-CALLFBI (225-5324) or a local FBI office;
- ▶ the Internet Crime Compliant Center (IC3) (particularly if a firm is trying to recall a wire transfer to a destination outside the United States); and local state securities regulators.<sup>10</sup>

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers should immediately notify by telephone an appropriate law enforcement authority.<sup>11</sup>

## Endnote

1. See FINRA Rule 11870(b)(1) and Rule 11870(d); see also NSCC Rule 50, Section 5.
2. See FINRA Rule 11870(e)). Note that some assets may be exempt from this timeframe. See FINRA Rule 11870(j).
3. Some transfers may occur outside of ACATS. See Rule 11870(a)(2). This *Notice* focuses on the transfers that occur within ACATS.
4. See, e.g., FINRA Rule 11870.03 (Sample Transfer Instruction Form). See also DTCC ACATS User Guide (August 2, 2022) (ACATS User Guide) (listing the information the ACATS system sources from the TIF that includes receiving and deliverer (*i.e.*, carrying) broker-dealer; customer name; customer account number; Social Security numbers, among other data).
5. A synthetic identity may include legitimate Social Security numbers with false names, addresses and dates of birth. Without a clearly identifiable victim, a synthetic identity may go undetected for longer periods of time.
6. See [Regulatory Notice 20-13](#) (May 2020) (reminding firms to be aware of fraud during the pandemic). See also [Regulatory Notices 20-32](#) (September 2020) (reminding firms to be aware of fraudulent options trading in connection with potential account takeovers and new account fraud); [Regulatory Notice 21-14](#) (March 2021) (alerting firms to recent increase in ACH "Instant Funds" abuse); and [Regulatory Notice 21-18](#) (May 2021) (sharing practices firms use to protect customers from online account takeover attempts).
7. See FINRA Rule 3310(b) and 31 C.F.R. § 1023.220.
8. See FINRA Rule 3310(a) and 31 C.F.R. § 1023.320.
9. See FINRA Rule 3310(f) and 31 C.F.R. § 1023.210(a)(5).
10. See NASAA, [Contact Your Regulator](#) (providing contact information for state securities and provincial securities regulators and other resources those agencies provide).
11. Firms may call FinCEN's Hotline at (866) 556-3974.

©2022. FINRA. All rights reserved. Regulatory Notices attempt to present information to readers in a format that is easily understandable. However, please be aware that, in case of any misunderstanding, the rule language prevails.

# Regulatory Notice

20-13

## Heightened Threat of Fraud and Scams

### FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic

#### Summary

The COVID-19 pandemic is affecting most aspects of our society and daily lives, as well as the U.S. economy and markets. Events with such profound impact routinely create opportunities for financial fraud.

Firms and their associated persons should be aware of and take appropriate measures to address the increased risks and challenges presented during the COVID-19 pandemic. In addition to new scams focusing on COVID-19, previous scams may also find new life as fraudsters adapt to and exploit recent events and related vulnerabilities, especially those related to the remote working environment.

FINRA is committed to providing guidance, updates and other information to help stakeholders stay informed about the latest developments relating to COVID-19, which can be found on FINRA's [COVID-19/Coronavirus Topic Page](#).

FINRA will also continue to inform the industry on emerging cybersecurity trends and related frauds, and reminds firms to review resources on [FINRA's Cybersecurity Topic Page](#), which provides information on how firms can strengthen their cybersecurity programs.

Questions regarding this *Notice* should be directed to:

- ▶ Greg Ruppert, Executive Vice President, National Cause and Financial Crimes Detection Programs, Member Supervision, at (415) 217-1120 or [greg.ruppert@finra.org](mailto:greg.ruppert@finra.org); or
- ▶ Sam Draddy, Senior Vice President, Insider Trading and PIPEs Surveillance, Member Supervision, at (240) 386 5042 or [sam.draddy@finra.org](mailto:sam.draddy@finra.org).

#### Background and Discussion

FINRA urges firms and associated persons to be cognizant of the heightened threat of frauds and scams to which firms and their customers may be exposed during the COVID-19 pandemic. This *Notice* outlines four common scams—(1) fraudulent account openings and money transfers; (2) firm

May 5, 2020

#### Notice Type

- ▶ Special Alert

#### Suggested Routing

- ▶ AML
- ▶ Compliance
- ▶ Cybersecurity
- ▶ Financial Crimes Department
- ▶ Fraud Department
- ▶ Legal
- ▶ New Accounts
- ▶ Operations
- ▶ Registered Representatives
- ▶ Risk Management
- ▶ Senior Management

#### Key Topics

- ▶ Cybersecurity
- ▶ Fraud

#### Referenced Rules and Notices

- ▶ FINRA Rule 2090
- ▶ FINRA Rule 3110
- ▶ FINRA Rule 3310
- ▶ FINRA Rule 4512
- ▶ Information Notice 3/26/20
- ▶ Information Notice 4/29/19
- ▶ Regulatory Notice 09-64
- ▶ Regulatory Notice 12-05
- ▶ Regulatory Notice 19-18

imposter scams; (3) IT Help Desk scams; and (4) business email compromise schemes—and describes measures that firms and associated persons may take to mitigate related risks. This information pre-dates the COVID-19 pandemic but may be useful to firms since FINRA has observed that these threats persist in the current environment.

### I. Fraudulent Account Openings and Money Transfers

Some firms have reported an increase in newly opened fraudulent accounts, which may otherwise be hard to identify as a result of overall increases in new account openings. Firms should be aware that fraudsters are targeting firms offering online account opening and, perhaps especially, firms that recently started offering such services. These fraudsters may be taking advantage of the pandemic to use stolen or synthetic identities to establish accounts to divert congressional stimulus funds, unemployment payments or to engage in automated clearing house (ACH) fraud.<sup>1</sup>

#### Common Characteristics of Scams

The specific tactics fraudsters use may vary, but they typically involve some combination of the following steps:

- ▶ **Establishing the Account**—Using stolen or synthetic customer identity information to establish a new brokerage account;<sup>2</sup>
- ▶ **Funding the Account**—Funding the newly established brokerage account by:
  - ▶ using stolen bank account information (routing and account numbers) to transfer money from the customer's bank account to the newly established brokerage account;
  - ▶ effecting smaller dollar transfers via ACH or other online payment methods from the customer's bank account; or
  - ▶ diverting other customer funds directly to the fraudster's account (*e.g.*, diverting unemployment benefits); and
- ▶ **Exfiltrating Funds**—Rapidly moving deposited funds out of the brokerage account by, for example:
  - ▶ making ATM withdrawals or purchases on debit cards for the brokerage account; or
  - ▶ linking the brokerage account to a third-party bank account or an account at another financial institution that provides pre-paid debit card products and services and then transferring funds to that account.

FINRA has observed that, in some cases, fraudsters emailed firms a falsified voided check to verify the new bank account information. The falsified check included the real customer's home address and looked like a legitimate check for the customer's bank account.



### Selected Firm Practices

FINRA has observed firms implement the following practices to address risks relating to fraudulent account openings and money transfers:

- ▶ **Customer Identification Program<sup>3</sup>**—Firms that permitted the opening of accounts through electronic means used both documentary and non-documentary methods to verify the identity of customers, including:
  - ▶ documentary identification (which included unexpired government-issued identification bearing a photograph, such as drivers' licenses or passports); and
  - ▶ non-documentary methods (which included contacting the customer; independently verifying the customer's identity with information obtained from a consumer reporting agency, public database or other source; checking references with other financial institutions; or obtaining a financial statement).
- ▶ **Monitoring for Fraud During Account Opening**—Firms used the following methods at the time of account opening to identify potential fraud:
  - ▶ limiting automated approval of multiple accounts opened by a single customer;
  - ▶ reviewing account application fields—such as telephone number, address, email address, bank routing numbers and account numbers—for repetition or commonalities among multiple applications, but with different customer names or identifiers; and
  - ▶ using technology to detect indicators of automated scripted attacks in the digital account application process (*e.g.*, extremely rapid completion of account applications).

Although some firms use micro-deposits as a mean to verify accounts, FINRA notes that other firms are concerned that fraudsters can undermine the utility of this verification method by using social engineering attacks to take over customer accounts at institutions across the financial services industry. As a result, and as discussed further below, these firms carefully watch for rapid withdrawals from accounts that were verified using micro-deposits.

- ▶ **Bank Account Verification and Restrictions on Fund Transfers**—Firms confirmed customers' identities with banks and restricted fund transfers in certain situations by, for example:
  - ▶ reviewing the IP address of transfer requests made online or through a mobile device to determine if the request was made from a location that is consistent with the customer's home address or locations from which the firm has previously received legitimate customer communications;

- ▶ verifying that the identity on the source account for fund transfers matches the customer's identity at the broker-dealer;
  - ▶ confirming that the identity of the destination bank account for cash transfers matches the customer's identity at the broker-dealer;
  - ▶ prohibiting the rapid transfer of recently deposited customer funds from customers' brokerage accounts to third party bank accounts (where some firms used risk criteria—*e.g.*, the amount of the transfer in dollar terms—to trigger reviews of transfer requests) by requiring a holding period (which allowed time for the filing of an ACH fraud report by the originating bank);
  - ▶ implementing a process for customers to obtain exceptions to these restrictions, which required them to complete additional steps to verify their account information, the transfer amount and their identity (such as through the use of third-party providers that leverage customers' credit bureau or other information); and
  - ▶ creating notifications for changes to bank account information that were sent to the customer via email, text message or instant message—as well as their official street address of record—informing them about the newly established linked bank account and asking them to call the firm if they have any questions.
- ▶ **Ongoing Monitoring of Accounts**—Firms continued to evaluate existing accounts for fraud risks where the accounts:
- ▶ were inactive, unfunded and soon to be restricted or closed; and
  - ▶ had losses related to credit extensions and were about to be placed into collections or write-off categories.
- ▶ **Collaborating with Clearing Firms**—Firms clearly understood the allocation of responsibilities between clearing and introducing firms for handling ACH transactions and implemented policies and procedures to meet those responsibilities effectively, including:
- ▶ defining how instructions related to ACH requests should be conveyed; and
  - ▶ understanding the responsible staff at the introducing firm who were authorized to transmit instructions to the clearing firm.
- ▶ **Suspicious Activity Report (SAR) Filing Requirements<sup>4</sup>**—Firms confirmed that ACH fraud was covered by their SAR procedures and reported them to the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN).

### Relevant Regulatory Obligations

In addition to considering the practices noted above, FINRA encourages firms to assess their compliance programs relating to account opening and money transfers and reminds them to review their policies and procedures related to:

- ▶ new account openings to confirm they comply with FINRA Rules [2090](#) (Know Your Customer) and [4512](#) (Customer Account Information), as well as the Bank Secrecy Act and its implementing regulations addressed under FINRA Rule [3310](#) (Anti-Money Laundering Compliance Program);
- ▶ handling of ACH transfer requests to “determine the authenticity of transmittal instructions”<sup>5</sup> obligations pursuant to FINRA Rule [3110](#) (Supervision);
- ▶ safeguarding customer “records and information” pursuant to Regulation S-P Rule 30;<sup>6</sup> and
- ▶ filing SARs with FinCEN.<sup>7</sup>

### Firm Imposter Scams

The expanded use of remote offices and telework arrangements may increase opportunities for fraudsters to impersonate firms and associated persons in communicating with customers or creating a fake online presence or websites.<sup>8</sup> As part of this scam, fraudsters may seek to obtain—via a website, email, text or other communications—customers’ personal information, including account information, or trick them into making investments or transferring funds. In some cases, fraudsters may seek to reduce the likelihood that customers will realize they have been the target of a fraud by directing them not to contact the firm by phone due to long wait times.

FINRA has observed firms using a variety of methods to address risks related to imposter scams, including:

- ▶ providing staff with training or fraud alerts describing firm imposter scams and the steps associated persons can take to protect the firm and its customers;
- ▶ alerting customer-facing staff that fraudsters may use the increase in remote work to engage in social engineering schemes against associated persons and advise them to vet incoming calls purporting to be from known customer numbers—for example by arranging a video call or asking customers questions where only the customers and their registered representative would know the answer; and
- ▶ implementing the practices discussed in FINRA [Information Notice 4/29/19](#) when they become aware of imposter websites.

### IT Help Desk Scams

Remote work arrangements also may increase the opportunity for social engineering attacks involving firms' IT Help Desks. In one variant of these attacks, fraudsters pose as associated persons and contact a firm's IT Help Desk to, for example, request a password reset. The fraudsters may use the conversation with the IT Help Desk staff to gain information about a firm's technical infrastructure or business operations, which they subsequently use to attack the firm, for example, by infiltrating the firm's network and possibly stealing funds from the firm.<sup>9</sup>

FINRA has observed firms address risks relating to such scams by training their IT Help Desk staff to verify callers' identities by, for example, asking for employees' identification numbers or other firm-specific information that would be challenging for fraudsters to obtain.

In a second variant of these attacks, fraudsters pose as a member of a firm's IT Help Desk team and contact associated persons in an attempt to harvest user credentials or introduce malware into the associated person's computer, which may then be used to steal credentials, confidential customer or firm data or other valuable information.

FINRA has observed firms address this risk by training associated persons to take extra precautions when receiving unsolicited calls or emails that appear to come from their firm's IT Help Desk, especially if the caller or email asks the associated person to click a link, enter a web address or download software to their computer. Some firms ask employees receiving such calls or emails not to respond and to call back the IT Help Desk on its official number to confirm the veracity of the original communication. In addition, they ask employees to report any suspicious activity to the firm so it can alert other staff that they may be targeted.

### II. Business Email Compromise Schemes<sup>10</sup>

Fraudsters may also take advantage of remote working environments to pose, via email or text message, as firm leadership to request one or more fund transfers, for example, related to accounts payable invoices. In another variant on this scam—the gift card procurement scam—fraudsters purporting to be a manager or executive email a subordinate with an urgent request for them to secretly purchase gift cards as a motivational award or one-time surprise for staff.

FINRA has observed firms addressing such risks by alerting staff that can disburse firm funds to:

- ▶ monitor for potential red flags of scams, such as requests arriving at an unusual time of day, using atypical language or greetings, requesting a transfer to a new account, requiring privacy or secrecy for the transactions or displaying unusual urgency; and
- ▶ confirm the request via telephone prior to acting on any requests, especially those sent via email channels.

FINRA has also observed firms address such risks by including an “external” banner to highlight emails received from outside the firm.

### Reporting Fraud

Although there may not be a regulatory requirement to report every incident described in this Notice, FINRA urges firms to protect customers and other firms by immediately reporting scams and any other potential fraud to:

- ▶ FINRA’s [Regulatory Tip Form](#) found on [FINRA.org](#) or through [FINRA’s Whistleblower Tip Line](#) at (866) 96-FINRA or [whistleblower@finra.org](mailto:whistleblower@finra.org);
- ▶ U.S. Securities and Exchange Commission’s tips, complaints and referral system ([TCRs](#)) or by phone at (202) 551-4790;
- ▶ the Federal Bureau of Investigation’s (FBI) tip line at 800-CALLFBI (225-5324) or a local FBI office;
- ▶ for cyber crimes, the [Internet Crime Compliant Center \(IC3\)](#) (particularly if a firm is trying to recall a wire transfer to a destination outside the United States); and
- ▶ local state securities regulators.<sup>11</sup>

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers *must* immediately notify by telephone an appropriate law enforcement authority in addition to filing a timely SAR. The firm may call FinCEN’s Hotline at (866) 556-3974.

## Endnotes

1. A synthetic identity includes legitimate Social Security numbers (SSNs) with false names, addresses and dates of birth. Without a clearly identifiable victim, it may go undetected for longer periods of time.
2. In some cases, fraudsters have also established a new account at a firm where a legitimate customer already has an account and used at least some elements of that customer's identity to establish the new account.
3. See 31 C.F.R. 1023.220 (setting forth requirements for customer identification programs for broker-dealers).
4. See 31 C.F.R. 1023.320 (setting forth SARs reporting requirements).
5. See [Regulatory Notice 12-05](#) (Verification of Email Instructions to Transmit or Withdraw Assets From Customer Accounts) and [Regulatory Notice 09-64](#) (Customer Assets).
6. Rule 30 under Regulation S-P requires firms 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. Regulation S-P also requires firms to provide initial and annual privacy notices to customers describing information sharing policies and informing customers of their right to opt-out of information sharing. Further, FINRA Rule [3110](#) (Supervision) requires firms to establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, including Rule 30 under Regulation S-P, and with applicable FINRA rules.
7. See [Regulatory Notice 19-18](#) (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations).
8. See FINRA [Information Notice 4/29/19](#) (Imposter Websites Impacting Member Firms).
9. See FINRA [Information Notice 3/26/20](#) (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19)).
10. See [FBI Release: FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic](#) (April 6, 2020).
11. See [www.nasaa.org/contact-your-regulator/](http://www.nasaa.org/contact-your-regulator/) (providing contact information for state securities regulators).

# Regulatory Notice

21-18

## Cybersecurity

### FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts

#### Summary

FINRA has received an increasing number of reports regarding customer account takeover (ATO) incidents, which involve bad actors using compromised customer information, such as login credentials (*i.e.*, username and password), to gain unauthorized entry to customers' online brokerage accounts.

To help firms prevent, detect and respond to such attacks, FINRA recently organized roundtable discussions with representatives from 20 firms of various sizes and business models to discuss their approaches to mitigating the risks from ATO attacks.

This *Notice* outlines the recent increase in ATO incidents; reiterates firms' regulatory obligations to protect customer information; and discusses common challenges firms identified in safeguarding customer accounts against ATO attacks, as well as practices they find effective in mitigating risks from ATOs—including recent innovations—which firms may consider for their cybersecurity programs.

This *Notice* does not create new legal or regulatory requirements, or new interpretations of existing requirements. A firm's cybersecurity program should be reasonably designed and tailored to the firm's risk profile, business model and scale of operations. There should be no inference that FINRA requires firms to implement any specific practices described in this *Notice*.

Questions regarding this *Notice* should be directed to:

- ▶ David Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or by [email](#); or
- ▶ Greg Markovich, Senior Principal Risk Specialist, Member Supervision, at (312) 899-4604 or by [email](#).

May 12, 2021

#### Notice Type

- ▶ Special Alert

#### Suggested Routing

- ▶ Compliance
- ▶ Information Technology
- ▶ Legal
- ▶ Operations
- ▶ Risk Management
- ▶ Senior Management

#### Key Topics

- ▶ Access Control
- ▶ Authentication
- ▶ Cybersecurity
- ▶ Fraud

#### Referenced Rules & Notices

- ▶ FINRA Rule 2090
- ▶ FINRA Rule 3110
- ▶ FINRA Rule 3310
- ▶ FINRA Rule 4512
- ▶ Information Notice 10/15/20
- ▶ Notice to Members 05-48
- ▶ Regulatory Notice 20-13
- ▶ Regulatory Notice 20-30
- ▶ Regulatory Notice 20-32



## Background and Discussion

FINRA has received an increasing number of reports regarding ATO incidents, which involve bad actors using compromised customer information, such as login credentials, to gain unauthorized entry to customers' online brokerage accounts. In addition, we have received reports regarding attackers using synthetic identities to fraudulently open new accounts; some of the information addressed here, particularly regarding the opening of online accounts, may help firms mitigate risks in this area.<sup>1</sup>

Customer ATOs have been a recurring issue, but reports to FINRA about such attacks have increased as more firms offer online accounts, and more investors conduct transactions in these accounts, in part due to the proliferation of mobile devices and applications (*i.e.*, "apps")<sup>2</sup> and the reduced accessibility of firm's physical locations due to the COVID-19 pandemic.

Bad actors have taken advantage of these conditions to attempt customer ATOs, often through common attack methods such as phishing emails and social engineering attempts (*e.g.*, fraudsters calling customers, pretending to be registered representatives from customers' firms to acquire their personal information).<sup>3</sup> Other reasons for this increase in attempts may include the large number of stolen customer login credentials available for sale on the "dark web" (*see* Appendix for definitions of cybersecurity terms used in this *Notice*) and the emergence of more sophisticated ATO methods, such as tools that automate ATO attacks at scale (*e.g.*, using mobile emulators to mimic mobile devices that have been compromised to access thousands of online brokerage accounts).

### Password Managers for Customer Account Protection

Some firms observed that customers often use the same login information across multiple accounts, making them particularly susceptible to ATOs conducted on a widescale (*e.g.*, credential stuffing).

To mitigate this threat, some firms recommend that customers use a password manager—an application that protects online accounts by suggesting and saving individual, strong passwords for each login. The password manager then automatically fills in the password whenever customers access their accounts online.

## Regulatory Obligations

FINRA reminds member firms of their obligations to protect sensitive customer data, as well as verify the identity and know the essential facts concerning every customer:

Regulatory Obligation	Summary
<a href="#">FINRA Rule 2090</a> (Know Your Customer)	Firms must use reasonable diligence, in regard to the opening and maintenance of every account, to know the “essential facts” concerning every customer. Essential facts are those required to: (1) effectively service the customer’s account; (2) act in accordance with any special handling instructions for the account; (3) understand the authority of each person acting on behalf of the customer; and (4) comply with applicable laws, rules and regulations.
SEC Regulation S-P, Rule 30	Firms must 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 ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of customer records and information; and protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.
SEC Regulation S-ID	Firms must develop and implement a written program to detect, prevent and mitigate identity theft in connection with the opening or maintenance of “covered accounts.” <sup>4</sup> In designing those programs, firms should consider, among other things, the methods of accessing covered accounts and the detection of red flags of identity theft in connection with authenticating customers.
Customer Identification Program (CIP)	Firms’ anti-money laundering compliance programs must establish, document and maintain a written Customer Identification Program (CIP). <sup>5</sup> Among other requirements, firms’ CIPs must include risk-based procedures that enable firms to form a reasonable belief that they know the true identity of each person that opens a new account. These procedures must be based on an assessment of the relevant risks, including those presented by the various types of accounts maintained by the firm and the various methods of opening accounts. <sup>6</sup> The CIPs must also describe when they will use documentary, non-documentary or a combination of both methods for identity verification. <sup>7</sup>

FINRA also encourages firms to assess their compliance programs related to new account openings and funds transfers, and review their policies and procedures related to:

- ▶ confirming that new account openings comply with [FINRA Rule 4512](#) (Customer Account Information), as well as the Bank Secrecy Act and its implementing regulations addressed under [FINRA Rule 3310](#) (Anti-Money Laundering Compliance Program);
- ▶ handling of ACH and other transmittal requests to “determine the authenticity of transmittal instructions” obligations pursuant to [FINRA Rule 3110](#) (Supervision); and
- ▶ filing Suspicious Activity Reports (SARs)<sup>8</sup> with FinCEN.<sup>9</sup>

## Common Challenges to Protecting Customer Accounts

During the roundtable discussions with FINRA, firms discussed the following cybersecurity challenges<sup>10</sup> they have encountered when safeguarding customer accounts from ATOs:

- ▶ identifying effective methods of verifying the identities of customers who establish accounts online;<sup>11</sup>
- ▶ addressing increased volume of attempted customer ATOs;
- ▶ preventing bad actors from transferring money in and out of customer accounts;
- ▶ identifying when bad actors have taken over customer accounts by modifying customers’ critical account information (e.g., email address, bank information) and are attempting fraudulent transactions;
- ▶ identifying when login attempts and requests to reset account passwords are actually made by a bad actor who has taken over a customer’s email account; and
- ▶ balancing security and customer experience considerations.

## Noted Practices

During the roundtable, firms discussed a variety of policies, procedures, controls and related tools to mitigate ATO-related risks. The firms typically used a risk-based approach to validating new customers’ identities, authenticating logins to firm systems and performing customer-requested actions (e.g., transactions in an account), coupled with strong back-end monitoring and robust procedures to respond quickly to identified customer ATOs.

### Verifying Customers’ Identities When Establishing Online Accounts

As part of their cybersecurity programs, firms that onboard customers online verified potential customers’ identities by:

- ▶ validating identifying information or documents that applicants provide (e.g., Social Security number (SSN), address, driver’s license), including, for example, through “likeness checks”; and

- ▶ asking applicants follow-up questions or requesting additional documents to validate their identities, based on information from credit bureaus, credit reporting agencies or firms providing digital identity intelligence (e.g., automobile and home purchases).

Alternatively, some firms contracted with third-party vendors to perform the above functions, as well as provide additional support (e.g., a database to verify the legitimacy of suspicious information in customers' applications).<sup>12</sup>

### Authenticating Customers' Identities During Login Attempts

Firms took a variety of approaches to validating the identities of customers when they access their online accounts:

**Multifactor authentication:** Most firms embraced multifactor authentication (MFA) as a key control that significantly reduces the likelihood that bad actors can take over a customer's account. Some of these firms required all customers to use MFA; others required customers to use MFA if their account had been compromised, while others simply encouraged customers to adopt it.

**Key takeaway:** *While not a "silver bullet," most participants believe MFA is currently one of the best ways to protect customers' accounts from ATOs.*

Unlike single-factor authentication (e.g., a password), MFA uses two or more different types of factors or secrets—such as a password and code sent via a Short Message Service (SMS) text message or an authentication app—which significantly reduces the likelihood that the exposure of a single credential will result in account compromise.<sup>13</sup> A number of firms are encouraging customers to adopt MFA by establishing streamlined MFA methods, such as customers entering their login credentials on trusted devices.

**Adaptive authentication:** Some firms use adaptive authentication techniques to further increase the security of customers' accounts. Adaptive authentication typically assesses both:

- ▶ the risk associated with a customer's login (i.e., the authentication system's confidence in the customer's identity, based on various factors associated with the login attempt (such factors are discussed further below)); and
- ▶ the risk of the activity the customer wishes to perform (e.g., checking an account balance or initiating a money transfer).

In situations where the authentication system assesses that at least one of these risks exceeds a certain risk threshold, the system will require the customer to provide additional information to confirm their identity. For example, a customer may be required to provide additional information to verify their identity if they:

- ▶ attempt to log in to their account from a new device or different location than usual; or
- ▶ seek to execute a higher risk transaction such as an abnormally large withdrawal or purchase of a different type of security (*e.g.*, a low-priced unlisted security) than usual, or change a bank account or email address associated with their account.

A risk threshold can be set in a variety of ways. For example, a firm may set relatively simple rules (*e.g.*, transactions exceeding a specific dollar value or percent of account size). Alternatively, a firm may establish policies that assess a broad range of factors to determine whether additional verification is required.

**Supplemental authentication factors:** There are a variety of factors that firms and vendors may incorporate into their authentication system and processes to verify a customer's identity, including:

- ▶ SMS text message codes;
- ▶ phone call verifications;
- ▶ media access control (MAC) addresses;
- ▶ geolocation information;
- ▶ third-party authenticator apps; and
- ▶ biometrics.

In addition, many firms noted they have transitioned away from using email addresses as authentication factors, due to the prevalence of email account breaches by bad actors.

### Back-End Monitoring and Controls

Firms conducted ongoing surveillance of both individual customer accounts and across these accounts to prevent, detect and mitigate ATO threats. (In some cases, the results of such back-end monitoring may feed back into firms' front-end controls.) This included, for example:

- ▶ monitoring at the customer account level for anomalies, such as:
  - ▶ indications of ATO attempts at the login level (*e.g.*, significant increases in number of failed logins in a brief time period for a specific account); and
  - ▶ account activity that could indicate that an ATO has occurred (*e.g.*, large purchases shortly after account opening; changes in email account of record followed by a request for a third-party wire; frequent transfers of funds in and out of an account);

- ▶ monitoring across customers' accounts for indications of credential stuffing or other large-scale attacks (*e.g.*, significant increases in the number of login attempts and failed logins across a large number of accounts);
- ▶ monitoring emails received from customers for red flags of social engineering (*e.g.*, problems with grammar or spelling; unexpected attachments, apps or links);<sup>14</sup>
- ▶ establishing back-end controls to prevent bad actors from moving money out of customer accounts, such as requiring a confirmation phone call with the customer using an established phone number when suspicious activity is detected in their account (*e.g.*, withdrawing money from an online brokerage account into a newly-established bank account); and
- ▶ scanning the dark web for keywords or data that could be useful to bad actors in facilitating an ATO (*e.g.*, firm name, customer account numbers, names of firm executives, planted accounts and passwords).

#### Procedures for Potential or Reported Customer ATOs

Firms discussed methods to proactively address potential or reported customer ATOs by:

- ▶ establishing a dedicated fraud group to investigate customer ATOs;
- ▶ responding promptly and effectively to customers who report ATOs, frequently updating them on their account status and minimizing the amount of time their accounts are locked or their trading ability is suspended;
- ▶ reviewing all of a customer's accounts at the firm for signs of problematic activity, if such activity is identified in one of their accounts;
- ▶ providing a method for customers to quickly communicate with someone at the firm, typically through voice or chat channels in a contact center; and
- ▶ reminding customers of recommended security practices (*e.g.*, MFA adoption).

#### Automated Threat Detection

Firms used a variety of automated processes to detect potential malicious actions by bad actors, for example, by:

- ▶ using web application firewalls (WAFs) and internally built tools to stop credential stuffing attacks;
- ▶ isolating suspicious IPs in a "penalty box"; and
- ▶ instituting geographic-based controls (*e.g.*, "impossible travel" or disallowing connections from countries where no customers reside).

### Restoring Customer Account Access

Firms noted that secure practices to restore customers' account access—whether because a customer has forgotten their password or because they are otherwise locked out—in a timely fashion are essential. At the same time, however, the process must be well thought out and incorporate appropriate safeguards so that it does not itself become an avenue for ATOs. Practices firms noted in this regard included:

- ▶ implementing two-factor authentication for all password resets, for example, requiring input of a time-sensitive code sent to investors by SMS text message (several firms noted that sending a code via email can be risky because customers' email accounts may have been compromised, so firms using this approach may want to ask for additional confirming information, as described in the bullet below); and
- ▶ requiring customers to contact call centers, and answer security questions based on less commonly available information (*i.e.*, information less likely to be available through the dark web or a customer's social media posts, and provided by the credit bureaus or firms providing digital identity intelligence) to restore their account access.

### Investor Education

Firms noted that they educated and trained their customers on account security by:

- ▶ including cybersecurity-related materials in the client onboarding process;
- ▶ providing up-to-date cybersecurity information;
- ▶ including on the firm's website resources—such as alerts—that customers can opt in to receiving, such as email or SMS text messages for certain types of account activity; and
- ▶ adding educational content to statements of older investors.

### Reporting Fraud

FINRA urges firms to protect customers and other firms by immediately reporting scams and any other potential fraud to:

- ▶ FINRA's [Regulatory Tip Form](#) found on [FINRA.org](#);
- ▶ U.S. Securities and Exchange Commission's tips, complaints and referral system ([TCRs](#)) or by phone at (202) 551-4790;
- ▶ the Federal Bureau of Investigation's (FBI) tip line at 800-CALLFBI (225-5324) or a local FBI office;
- ▶ the [Internet Crime Complaint Center \(IC3\)](#) for cyber-crimes (particularly if a firm is trying to recall a wire transfer to a destination outside the United States); and
- ▶ local state securities regulators.<sup>15</sup>



In addition, firms should consider whether circumstances require that the firm file a SAR<sup>16</sup> or report pursuant to [FINRA Rule 4530](#) (Reporting Requirements).<sup>17</sup>

## Conclusion

As noted herein, FINRA has received reports that the prevalence and sophistication of customer ATOs have been increasing. In the face of this threat, firms have implemented a variety of policies, procedures, controls and related tools to prevent, detect and respond to ATOs. FINRA shares practices roundtable participants found to be effective to help other firms mitigate ATO risks. Additional information related to cybersecurity risk management can be found on FINRA's [Cybersecurity Topic Page](#).

## Appendix

The following list defines commonly-used cybersecurity terms that appear in this *Notice*:

<b>Biometrics</b> – the unique physical identifiers ( <i>e.g.</i> , fingerprint, voice and facial recognition) or behavioral characteristics ( <i>e.g.</i> , mouse activity and keyboard strokes on computers; touchscreen behavior and device movement on mobile devices) humans display to digitally authenticate their identity.
<b>Credential Stuffing</b> – a cyberattack in which a bad actor uses a large set of illegally-acquired usernames and passwords to attempt to gain unauthorized access to multiple user accounts.
<b>Dark Web</b> – the portion of the Internet that can only be accessed through special types of software and is often used to anonymously conduct illegal activity.
<b>Impossible Travel</b> – a security control that compares the locations of a user’s most recent two sign-in attempts to determine if travel between those locations was impossible in the timeframe given ( <i>e.g.</i> , logging in from Cleveland, Ohio and then, twenty minutes later, from Salt Lake City, Utah).
<b>Likeness Check</b> – an identity verification method where applicants upload a photo or video of themselves, which is then compared with their recently submitted identity documents (and, at times, voice recordings).
<b>Media Access Control (MAC)</b> – a unique identifier used to identify a specific hardware device at the network level.
<b>Penalty Box</b> – a tool that isolates Internet Protocol (IP) addresses that exhibit potentially malicious behavior.
<b>Planted Account</b> – a fake account established by a firm within its customer database. In the context of cybersecurity, firms often monitor the dark web for information related to planted accounts to uncover data breaches.
<b>Short Message Service (SMS)</b> – a system for sending short messages ( <i>e.g.</i> , text) over a wireless network.
<b>Trusted Device</b> – a device frequently used by a customer to access their online account, such as a mobile phone, tablet or home computer. A customer can designate a device as “trusted” on the Verification Code screen by clicking the box next to “Don’t ask again on this computer”.
<b>Web Application Firewall (WAF)</b> – a firewall that monitors traffic between a web application and the Internet and filters out any malicious traffic (as defined by its set of policies).

## Endnotes

1. See [Regulatory Notice 20-32](#) (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud) for definitions of ATOs and synthetic identities.
2. See FINRA's [2018 Report on Selected Cybersecurity Practices](#) for effective practices firms have implemented to protect sensitive firm and customer information as the use of mobile devices expands and becomes more widespread.
3. See [Regulatory Notice 20-30](#) (Fraudsters Using Registered Representatives Names to Establish Imposter Websites).
4. See 17 CFR 248.201(b)(3), which defines "covered account" as:
  - (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a brokerage account with a broker-dealer or an account maintained by a mutual fund (or its agent) that permits wire transfers or other payments to third parties; and
  - (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.
5. See 31 C.F.R. 1023.220 and 31 C.F.R. 1023.100(d). Pursuant to FINRA Rule 3310(b), firms must establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and its implementing regulations, including the CIP Rule.
6. *Ibid.*
7. See 31 C.F.R. 1023.220(a)(2)(ii). For firms relying on documents to verify identity, the documents utilized may include an original unexpired government-issued identification evidencing nationality or residence and bearing a photograph, such as a driver's license or passport. Non-documentary methods of verifying customer identity under the CIP Rule may include contacting a customer; independently verifying the customer's identity through comparison of the information the customer provides with information from a consumer reporting agency, public database, or other source; checking references with other financial institution; or obtaining a financial statement.
8. See 31 C.F.R. 1023.320 for SARs reporting requirements.
9. See FinCEN's July 2020 [Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 \(COVID-19\) Pandemic](#) for additional guidance on filing SARs.
10. The challenges discussed in this *Notice* may require firms to address regulatory obligations beyond the context of cybersecurity—for example, those related to anti-money laundering compliance programs.
11. See FinCEN's [July 2020 Advisory](#) and [Regulatory Notice 20-13](#) (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic) for recent, common tactics bad actors use to establish fraudulent customer accounts.

12. Outsourcing an activity or function to a third party does not relieve firms of their ultimate responsibility for compliance with all applicable securities laws and regulations and FINRA and MSRB rules regarding the outsourced activity or function. FINRA has provided substantial guidance regarding firms' responsibilities when outsourcing activities to third-party service providers. *See, e.g., [Notice to Members 05-48](#) (Members' Responsibilities When Outsourcing Activities to Third-Party Service Providers).*
13. *See [Information Notice 10/15/20](#) (Cybersecurity Background: Authentication Methods)* for a primer on authentication techniques for firms to consider implementing within their cybersecurity programs.
14. *See [FINRA's 2018 Cybersecurity Report](#)* for additional effective practices firms have implemented to mitigate the threat of phishing attacks.
15. *See* North American Securities Administrations Association's [Contact Your Regulator](#).
16. *See supra* note 9. *See also* FinCEN's [Frequently Asked Questions \(FAQs\) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports \(SARs\)](#).
17. For additional information about the requirements of FINRA Rule 4530 (Reporting Requirements), *see* [Rule 4530 Frequently Asked Questions](#).

**FINANCIAL INDUSTRY REGULATORY AUTHORITY  
LETTER OF ACCEPTANCE, WAIVER AND CONSENT  
NO: 2006004297301**

TO: Department of Enforcement  
Financial Industry Regulatory Authority ("FINRA")

RE: E\*Trade Securities, LLC (CRD No. 29106) and  
E\*Trade Clearing, LLC (CRD No. 25025)

Pursuant to Rule 9216 of FINRA's Code of Procedure, Respondents E\*Trade Securities, LLC and E\*Trade Clearing, LLC (collectively "E\*Trade," "Firm," or "Respondent") submit this Letter of Acceptance, Waiver and Consent ("AWC") for the purpose of proposing a settlement of the alleged rule violations described below. This AWC is submitted on the condition that, if accepted, FINRA will not bring any future actions against E\*Trade alleging violations based on the same factual findings described herein.

**I.**

**ACCEPTANCE AND CONSENT**

- A. Respondent hereby accepts and consents, without admitting or denying the findings, and solely for the purposes of this proceeding and any other proceeding brought by or on behalf of FINRA, or to which FINRA is a party, prior to a hearing and without an adjudication of any issue of law or fact, to the entry of the following findings by FINRA:

**BACKGROUND**

Respondent E\*Trade Securities, LLC has been a registered broker-dealer and a member of FINRA (f/k/a National Association of Securities Dealers or NASD) since February 19, 1992. E\*Trade Securities' principal place of business is New York, New York. The Firm's business primarily consists of providing an on-line, Internet-based platform for customers trading in stocks and options.

E\*Trade Clearing, LLC has been a registered broker-dealer and a member of FINRA since April 2002. E\*Trade Clearing's principal place of business is also New York, New York. The activities of E\*Trade Clearing, as reflected by its name, are primarily related to clearing and are not sales related.

RECEIVED  
2006 DEC 31 A 11:09  
REGISTRATION & DISCLOSURE

## **OVERVIEW**

During most of the period of January 1, 2003 through May 31, 2007 (the "review period"), E\*Trade primarily utilized an automated proprietary system (the "System") to review accounts for potentially suspicious activity. The System employed five filters which queued transactions and accounts for further review by a group of analysts within the Firm's AML/Risk Department. The Firm developed these filters by identifying patterns of abnormal activity in brokerage accounts surrounding money movement. Consequently, E\*Trade's AML filter-based System triggered a review of potentially suspicious trading activity primarily when accompanied by money movement activity. Because the Firm's AML System did not flag and cause the review of accounts for suspicious trading activity unless accompanied by suspicious money movement, it was not reasonably designed to achieve compliance with the Bank Secrecy Act and implementing regulations thereunder, in contravention of NASD Conduct Rule 3011(b), and the Firm's written procedures for detecting and reporting suspicious trading activity did not comply with NASD Conduct Rule 3011(a). Since E\*Trade is a registered municipal securities dealer, E\*Trade also violated MSRB Rule G-41. E\*Trade's violations of NASD Rule 3011 and MSRB Rule G-41 also constitute a violation of NASD Rule 2110.

## **LEGAL STANDARD AND FACTS**

### **A. FINRA's AML Rule**

On July 2, 2002, the Department of Treasury, in implementing the Bank Secrecy Act, issued the regulation requiring suspicious transaction reporting for broker-dealers.<sup>1</sup> In accordance with this regulation, FINRA promulgated Rule 3011, which since 2002 has required broker-dealers to, among other things,

(a) Establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g) of the Bank Secrecy Act and the implementing regulations thereunder;

(b) Establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder;<sup>2</sup>

---

<sup>1</sup> 31 C.F.R. §103.19(a)(1) (2002).

<sup>2</sup> NASD Conduct Rule 3011; *see also* Special NASD Notice to Members 02-21, *Anti-Money Laundering*, dated April 2002, at 5.

\*\*\*

A firm's AML procedures must address a number of areas including monitoring of account activities, including but not limited to, *trading* and the flow of money into and out of accounts.<sup>3</sup> Firms are required to file with Treasury's Financial Crimes Enforcement Network ("FinCEN") "a report of any suspicious transaction relevant to a possible violation of law or regulation."<sup>4</sup> With respect to the monitoring of trading, FinCEN's SAR-SF identifies 20 types of suspicious activity that must be reported including "market manipulation," "pre-arranged or other non-competitive trading," and "wash or other fictitious trading."

A firm's obligation is not a one-size-fits-all requirement and each financial institution should tailor its AML program to fit its business. In this regard, each broker/dealer, in developing an appropriate AML program should consider factors such as its size, location, business activities, the types of accounts it maintains, and the types of transactions in which its customers engage.<sup>5</sup> One of the factors that members are instructed to consider generally when tailoring their supervisory procedures and systems to the business conducted is the technological environment in which the firm operates.<sup>6</sup> On-line firms such as E\*Trade have been instructed to "consider conducting computerized surveillance of account activity to detect suspicious transactions and activity."<sup>7</sup>

**B. E\*Trade's Automated AML System Was Inadequate Because It Focused Primarily on Money Movement**

Between January 2003 and May 2007, E\*Trade primarily relied upon an automated proprietary filter-based System to review accounts for money laundering activity. That System focused primarily on the review of suspicious money movement. The Firm's System utilized five filters that queued transactions and accounts for further review by analysts. Two of the five filters were designed to flag suspicious patterns of money movement into and out of accounts. Another two of the five filters were designed primarily to flag suspicious patterns of money movement in relation to the number or dollar value of trades executed. Only the fifth filter was focused primarily on potentially

---

<sup>3</sup> Special NASD Notice to Members 02-21 at 5 (stating, in relevant part, that firms must determine the manner in which AML procedures that address, among other things, "monitoring of account activities including but not limited to, trading and the flow of money into and out of the account," will apply to various accounts).

<sup>4</sup> 31 C.F.R. §103.19(a)(1) (2002).

<sup>5</sup> Special NASD Notice to Members 02-21 at 4.

<sup>6</sup> NASD Notice to Members 99-45, *NASD Provides Guidance On Supervisory Responsibilities*, at 2.

<sup>7</sup> Special NASD Notice to Members 02-21 at 7.



suspicious trading activity and that was limited to monitoring the trading activity within E\*Trade employees' accounts.

Once a filter was triggered, the transaction or account that resulted in the filter "hit" was electronically placed in the queue, resulting in a "System alert." Analysts then manually accessed a variety of other sources and systems to review the account activity, including any suspicious trading activity. These sources included internal systems, internet resources, FinCEN reports, and OFAC alerts from CDC. During the review period, there were approximately 400 to 800 System alerts each day and E\*Trade employed three to six analysts who were responsible for reviewing these alerts. Because the alerts were triggered by money movements, it was unlikely that the System analysts reviewed for suspicious trading activity, such as wash or matched trading, in the absence of money movements. Ordinarily, the System analysts only reviewed for potentially manipulative trading activity when they received such a System alert or a referral from another department in the Firm.

During the review period, E\*Trade processed, on average, more than 110,000 customer orders daily with little or no human intervention. During this period, E\*Trade did not tailor its suspicious activity monitoring program to its business of facilitating investors' self-directed electronic access to the market. For example, the Firm did not conduct computerized surveillance of customer account activity to monitor for matched or washed trading. Instead, it relied on its System analysts and other employees to manually monitor for and detect suspicious trading activity without providing them with sufficient automated tools necessary to monitor for such activity.

Such an approach to suspicious activity detection was unreasonable given E\*Trade's business model. By way of example, for a ten month period between January through October 2006, E\*Trade customers executed 85,029 matched transactions with the exact same share amount, price, and execution time. While matched trading is not illegal in and of itself, it is expressly prohibited when effectuated "[f]or purposes of creating a false or misleading appearance of active trading in any security[.]"<sup>8</sup> Consequently, a matched trade could be an indication of suspicious activity requiring further review.

E\*Trade, however, had no automated systems specifically designed to detect manipulative matched or wash trading. On-line trading firms, such as E\*Trade, are required to design and implement systems reasonably designed to detect trading activity in customer accounts that may be manipulative and thus reportable. Based upon the foregoing, E\*Trade violated NASD Conduct Rule 3011(b).

**C. E\*Trade's AML Policies And Procedures Violated  
NASD Conduct Rule 3011(a)**

---

<sup>8</sup> Securities Exchange Act of 1934 § 9(a)(1) (2002).

E\*Trade's AML procedures, called upon employees to view transactions in the context of other account activity to determine whether a transaction was suspicious. The AML procedures defined "transactions" to include "deposits, withdrawals, wire transfers, securities trading, and investments."<sup>9</sup> As described above, during the review period the Firm's AML filter-based System triggered review of potentially suspicious trading activity primarily when accompanied by money movement activity. Accordingly, during the review period, because the Firm did not have separate and distinct monitoring procedures for suspicious trading activity in the absence of money movement, E\*Trade's AML policies and procedures could not reasonably be expected to detect and cause the reporting of suspicious securities transactions.<sup>10</sup>

These failures constitute a violation of NASD Conduct Rule 3011(a).

### **Conclusion**

As set forth above, E\*Trade violated NASD Conduct Rules 3011 and 2110, and MSRB Rule G-41 (1) by failing to establish and implement policies and procedures that could reasonably be expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g), and (2) by failing to establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder.

B. Respondent also consents to the imposition, at a maximum, of the following sanctions:

1. A censure; and
2. A fine of \$1 million.

The sanctions imposed herein shall be effective on a date set by FINRA staff.

The sanctions set forth above take into account the Firm's prompt corrective action to remediate its AML system and procedures after the initiation of FINRA's investigation, but without prompting by FINRA, including the implementation of automated monitoring systems specifically designed to detect suspicious trading during the review period and the expansion of staff along with the retention of third party vendors dedicated to the monitoring function.

---

<sup>9</sup> E\*Trade Financial Corporation Domestic Regulated Brokerage Subsidiaries Anti-Money Laundering Policies And Procedures, *Transactions*, at 6 (emphasis added).

<sup>10</sup> Within the Firm's written supervisory procedures and manuals during the review period, there were a total of seven references to "market manipulation", but these were limited in nature and could not reasonably be expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g).

## **II.**

### **WAIVER OF PROCEDURAL RIGHTS**

Respondent specifically and voluntarily waives the following rights granted under FINRA's Code of Procedure:

- A. To have a Formal Complaint issued specifying the allegations against it;
- B. To be notified of the Formal Complaint and have the opportunity to answer the allegations in writing;
- C. To defend against the allegations in a disciplinary hearing before a hearing panel, to have a written record of the hearing made and to have a written decision issued; and
- D. To appeal any such decision to the National Adjudicatory Council ("NAC") and then to the U.S. Securities and Exchange Commission and a U.S. Court of Appeals.

Further, Respondent specifically and voluntarily waives any right to claim bias or prejudgment of the General Counsel, the NAC, or any member of the NAC, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including acceptance or rejection of this AWC.

Respondent further specifically and voluntarily waives any right to claim that a person violated the *ex parte* prohibitions of FINRA Rule 9143 or the separation of functions prohibitions of FINRA Rule 9144, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

## **III.**

### **OTHER MATTERS**

Respondent understands that:

- A. Submission of this AWC is voluntary and will not resolve this matter unless and until it has been reviewed and accepted by the NAC, a Review

Subcommittee of the NAC, or the Office of Disciplinary Affairs ("ODA"), pursuant to FINRA Rule 9216;

- B. If this AWC is not accepted, its submission will not be used as evidence to prove any of the allegations against the Firm; and
- C. If accepted:
  - 1. this AWC will become part of Respondent's permanent disciplinary record and may be considered in any future actions brought by FINRA or any other regulator against it;
  - 2. this AWC will be made available through FINRA's public disclosure program in response to public inquiries about the Firm's disciplinary record;
  - 3. FINRA may make a public announcement concerning this agreement and the subject matter thereof in accordance with NASD Rule 8310 and IM-8310-3; and
  - 4. Respondent may not take any action or make or permit to be made any public statement, including in regulatory filings or otherwise, denying, directly or indirectly, any finding in this AWC or create the impression that the AWC is without factual basis. Respondent may not take any position in any proceeding brought by or on behalf of FINRA, or to which FINRA is a party, that is inconsistent with any part of this AWC. Nothing in this provision affects Respondent's right to take legal or factual positions in litigation or other legal proceedings in which FINRA is not a party.
- D. Respondent may attach a Corrective Action Statement to this AWC that is a statement of demonstrable corrective steps taken to prevent future misconduct. Respondent understands that it may not deny the charges or make any statement that is inconsistent with the AWC in this Statement. This Statement does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA or its staff.

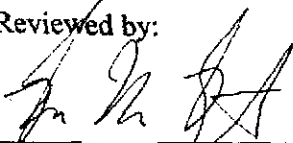
Respondent certifies that it has read and understands all of the provisions of this AWC and has been given a full opportunity to ask questions about it; that it has agreed to its provisions voluntarily; and that no offer, threat, inducement, or promise of any kind, other than the terms set forth herein and the prospect of avoiding the issuance of a Complaint, has been made to induce the Firm to submit it.

12-17-08  
Date

E\*Trade Securities, LLC  
E\*Trade Clearing, LLC  
Respondent  
E\*Trade Securities, LLC  
E\*Trade Clearing, LLC

By: James E. Ballowe, Jr.  
General Counsel

Reviewed by:

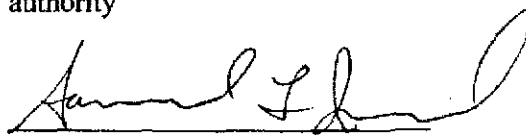


Bruce M. Bettigole  
Counsel For Respondent  
Mayer Brown LLP  
1909 K Street, N.W.  
Washington, D.C. 20006-1101

Accepted by FINRA:

12/31/08  
Date

Signed on behalf of the  
Director of ODA, by delegated  
authority



Samuel L. Israel  
Associate Vice President and Chief  
Counsel  
FINRA Department of Enforcement  
1801 K Street, N.W., Suite 800  
Washington, D.C. 20006-1334  
(t) 202-974-2868  
(f) 202-721-8316

**FINANCIAL INDUSTRY REGULATORY AUTHORITY**  
**LETTER OF ACCEPTANCE, WAIVER AND) CONSENT**  
**NO. 2007009026302**

TO: Department of Enforcement  
Financial Industry Regulatory Authority ("FINRA")

RE: Scottrade Inc. (CRD No. 8206)

Pursuant to Rule 9216 of FINRA's Code of Procedure, Respondent Scottrade Inc. ("Scottrade" or "Firm") submits this Letter of Acceptance, Waiver and Consent ("AWC") for the purpose of proposing a settlement of the alleged rule violations described below. This AWC is submitted on the condition that, if accepted, FINRA will not bring any future actions against Scottrade alleging violations based on the same factual findings described herein.

**I.**

**ACCEPTANCE AND CONSENT**

- A. Respondent hereby accepts and consents, without admitting or denying the findings, and solely for the purposes of this proceeding and any other proceeding brought by or on behalf of FINRA, or to which FINRA is a party, prior to a hearing and without an adjudication of any issue of law or fact, to the entry of the following findings by FINRA:

**BACKGROUND**

Scottrade has been a registered broker dealer and member of FINRA (f/k/a National Association of Securities Dealers or NASD) since May 23, 1980. The Firm's principal place of business is St. Louis, Missouri. It has more than 400 branch offices throughout the country and employs approximately 1,300 registered representatives. The Firm is an on-line discount broker-dealer. Its primary business consists of providing an on-line platform for customers to enter orders for trading stocks, including those traded on the NYSE, the Nasdaq, the Over-The-Counter Bulletin Board market ("OTCBB") and the Pink Sheets, listed options, fixed income securities and mutual funds. It is also a registered municipal securities dealer.

**OVERVIEW**

Since 2002, NASD Conduct Rule 3011 has required firms to establish and implement policies, procedures, and internal controls that can be reasonably expected to detect and cause the reporting of suspicious transactions as required by the Bank Secrecy Act and the implementing regulations thereunder. This includes suspicious securities transactions.

Scottrade is an on-line discount broker-dealer. Its primary business consists of providing an on-line platform for customers trading in securities. Scottrade's business model allows customers to open accounts on a non-face-to-face basis, has limited person-to-person customer

000011300 2009

relationships, offers a broad range of investment products, and provides customers with access to enter orders for securities on-line.

Between April 2003 and April 2008 (the "review period"), Scottrade failed to establish and implement AML policies, procedures, and internal controls that were reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder.

More specifically, between April 2003 through January 2005, Scottrade's AML policies, procedures, and internal controls were wholly inadequate to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder given the Firm's business model. During this time period, Scottrade failed to design and implement reasonable policies, procedures, and internal controls tailored to its business model. The Firm's AML monitoring was manual and relied exclusively on external sources and internal sources to refer potentially suspicious transactions to its AML Officer. The Firm did not provide adequate written guidance to its employees as to how to detect or review for potentially suspicious activity.

Until June 2004, Scottrade's AML Compliance Officer/Director of Risk Management was the only person specifically tasked with investigating the referrals. He investigated the referrals to determine whether any potentially suspicious money movement required reporting. In June 2004, the Firm hired one Risk Management Analyst to assist with this review. Despite the high volume of on-line trading at the Firm, Scottrade had no systematic or automated processes to monitor for potentially suspicious transactions and generate referrals to the Risk Management Department. Compounding the Firm's lack of internal controls was its failure to provide adequate written guidance in its procedures as to how to detect or review for potentially suspicious activities for escalation and reporting as appropriate.

It was not until February 2005, more than two years after Rule 3011 became effective, that Scottrade implemented a proprietary automated filter-based system (the "CARS System") to monitor for suspicious transactions. The CARS System utilized nine filters that queued transactions for further review by the Firm's AML analysts. In September 2006, the Firm implemented a proprietary volume exception report ("Analytics Volume Report") designed to detect pump-and-dump account intrusions and unauthorized trading activity resulting from such account intrusions. But even with the implementation of the CARS System and the Analytics Volume Report, the Firm's AML policies, procedures, and internal controls between February 2005 and April 2008 still were not designed to detect and cause the reporting of suspicious trading activity, unless such activity was accompanied by money movement. As a result, between February 2005 and April 2008, Scottrade's AML policies, procedures, and internal controls continued to be inadequate to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder because they were not reasonably designed to detect and cause the reporting of suspicious securities transactions.

By virtue of this conduct, Respondent Scottrade violated NASD Conduct Rules 3011(a) and (b) and 2110 and MSRB Rule G-41.

## **LEGAL STANDARD AND FACTS**

### **A. Anti-Money Laundering Requirements**

NASD Conduct Rule 3011, adopted on April 24, 2002 and amended on October 22, 2002, requires all member firms to "develop and implement a written anti-money laundering program reasonably designed to achieve and monitor the firm's compliance with the requirements of the Bank Secrecy Act (31 U.S.C. § 5311, *et seq.*), and the implementing regulations promulgated thereunder by the Department of the Treasury." Similarly, MSRB Rule G-41 requires every registered municipal securities dealer to "establish and implement an anti-money laundering compliance program reasonably designed to achieve and monitor ongoing compliance with the requirements of the Bank Secrecy Act, 31 U.S.C. 5311, *et seq.* and the regulations thereunder."

In April 2002, FINRA issued Notice to Members ("NTM") 02-21, which reminded broker-dealers that by April 24, 2002, they were required to establish and implement AML programs designed to achieve compliance with the Bank Secrecy Act and the regulations promulgated thereunder.<sup>1</sup> The Notice further advised broker-dealers that their AML procedures must address a number of areas including monitoring of account activities, "including but not limited to, trading and the flow of money into and out of accounts."<sup>2</sup>

Title 31 U.S.C. § 5318(g) authorizes the United States Department of the Treasury to issue suspicious activity reporting requirements for broker-dealers. The Treasury Department issued the implementing regulation, 31 C.F.R., § 103.19(a)(1) on July 1, 2002. It provided that, with respect to any transaction after December 30, 2002, "[e]very broker or dealer in securities within the United States . . . shall file with FinCEN . . . a report of any suspicious transaction relevant to a possible violation of law or regulation." Section (a)(2) of that regulation specifically provides:

A transaction requires reporting ... if it is conducted or attempted by, at, or through a broker-dealer, it involves or aggregates funds or other assets of at least \$5,000, and the broker-dealer knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

(i) Involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;

---

<sup>1</sup> Special NASD Notice to Members 02-21 at 5.

<sup>2</sup> *Id.*



(ii) Is designed, whether through structuring or other means, to evade any requirements of this part or of any other regulations promulgated under the Bank Secrecy Act, . . .;

(iii) Has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or

(iv) Involves use of the broker-dealer to facilitate criminal activity.

The Bank Secrecy Act's implementing regulations define "transaction," in relevant part as "...a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit or other monetary instrument, security, . . . or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected."

In August 2002, FINRA issued NTM 02-47, which set forth the final AML rules promulgated by the United States Department of the Treasury for the securities industry. This NTM further advised broker-dealers of their duty to file a SAR-SF for any suspicious transactions occurring after December 30, 2002.

Under NASD Conduct Rule 3011, firms are required to establish and implement policies, procedures, and internal controls that can be reasonably expected to detect and cause the reporting of suspicious transactions as required by the Bank Secrecy Act and the implementing regulations thereunder. This includes suspicious securities transactions irrespective of associated money movement.

A firm's obligation is not a one-size-fits-all requirement and each financial institution should tailor its AML program to fit its business. In this regard, each broker-dealer, in developing an appropriate AML program should consider factors such as its size, location, business activities, the types of accounts it maintains, and the types of transactions in which its customers engage.<sup>3</sup> In NTM 02-21, FINRA specifically instructed on-line firms such as Scottrade to "consider conducting computerized surveillance of account activity to detect suspicious transactions and activity."<sup>4</sup> This was consistent with prior FINRA guidance that one of the factors firms should consider when tailoring their supervisory procedures and systems to their business is the technological environment in which the firm operates.<sup>5</sup>

---

<sup>3</sup> Special NASD Notice to Members 02-21 at 4.

<sup>4</sup> *Id.* at 7.

<sup>5</sup> NASD Notice to Members 99-45, *NASD Provides Guidance On Supervisory Responsibilities*, at 2.

## **B. Scottrade's Business Model**

Scottrade's primary business consists of providing an on-line platform for customers trading in securities. Scottrade's business model allows customers to open accounts on a non-face-to-face basis, has limited person-to-person customer relationships, offers a broad range of investment products, and provides customers with access to enter orders for securities on-line. The Firm facilitated approximately 49,000 trades per day in 2003, approximately 76,000 daily trades in 2004, approximately 100,000 in 2005, approximately 120,000 in 2006 and approximately 150,000 in 2007. Among the inherent risks of this business model, and the sheer volume of transactions involved, are an increased risk of identity theft and account intrusions, and the use of customer accounts to launder money using securities or other instruments or to violate securities laws.

## **C. Scottrade's AML Policies, Procedures, And Internal Controls For Monitoring For Suspicious Transactions From April 2003 Through February 2005 Were Not Reasonable**

Between April 2003 and February 2005, the Firm's AML policies, procedures, and internal controls were inadequate to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder given the Firm's business model. During this time period, Scottrade failed to establish and implement reasonable AML policies, procedures, and internal controls tailored to its business model.

Despite the high volume of on-line trading at the Firm, Scottrade did not have any systematic or automated system designed to detect potentially suspicious money movement or securities transactions for further analysis and reporting as appropriate. Instead, the Firm used a manual system for monitoring its accounts for suspicious activities, which relied exclusively on internal sources, including branch, cashiering and margin personnel, and external sources, to refer potentially suspicious activity to the Risk Management Department for further review. The Firm did not provide adequate written guidance to its employees as to how to detect or review for potentially suspicious activity.

Furthermore, until June 2004, Scottrade's AML Compliance Officer/Director of Risk Management was the only person specifically tasked with investigating the referrals to determine whether the activity was suspicious activity that required reporting. In June 2004, the Firm hired one Risk Management Analyst to assist with this review. Scottrade's AML procedures failed to provide adequate written guidance to the Firm's personnel, including the AML Compliance Officer and the Risk Management Analyst, as to how to detect or review for suspicious activity. Their review of accounts for suspicious activity focused on reviewing for suspicious money movement into and out of accounts. During this time period, neither the AML Compliance Officer nor the Risk Management Analyst nor anyone else at Scottrade specifically monitored for potentially suspicious trading activity.

The sheer volume of on-line trading rendered the lack of an automated system, along with the Firm's reliance on inadequate internal resources to detect suspicious activity, unreasonable.

**D. From February 2005 Through April 2008, Scottrade's AML Policies, Procedures, And Internal Controls For Monitoring For Suspicious Securities Transactions Were Inadequate**

In February 2005, more than two years after Rule 3011 became effective, Scottrade implemented its CARS System, a proprietary, automated filter-based system to monitor for suspicious transactions. Originally, the CARS System was designed with nine filters that predominantly monitored for suspicious money movement. Through April 2008, the number of filters and the filters themselves were modified by Scottrade, but throughout this time period, all of the filters, except for two, were exclusively designed to detect suspicious money movement. The two exceptions were a filter designed to flag suspicious money movement in relation to the number of trades executed and a Penny Stock Filter, which was designed to monitor for potentially suspicious trading activity. The Penny Stock Filter, however, only generated an alert if there was money movement into or out of an account that independently triggered another filter.

In September 2006, the Firm implemented an Analytics Volume Report which was designed to detect pump-and-dump account intrusions and unauthorized trading activity resulting from such account intrusions. Absent indicia of a compromised account, the Analytics Volume Report was not utilized by the Firm to detect suspicious trading activity by *bona fide* account holders. In the summer of 2007, the Firm suspended its use of the Analytics Volume Report for a three month period.

Notwithstanding the implementation of the CARS System and the Analytics Volume Report, the Firm did not have adequate policies, procedures, and internal controls to detect and cause the reporting of suspicious securities transactions. Under the CARS System, when suspicious activity triggered one of the filters, it generated an alert to the Firm's AML analysts, who were responsible for investigating the alerts. The Firm's AML Analysts only reviewed the CARS System for potentially suspicious trading activity captured in a filter if there was money movement into or out of an account that independently triggered one of the filters. Between February 2005 and April 2008, an average of 1,300 alerts were generated monthly. The alerts were weighted and reviewed by the AML Analysts based upon the weighting priority of the alert. Not every alert was reviewed. Alerts that were not reviewed were archived.

Scottrade's AML procedures failed to provide adequate written guidance to its AML Analysts as to when and how they should review accounts for suspicious trading activity in connection with money movements. In February 2007, the Firm added a procedure for its AML Analysts, which stated, "Check account activity for any other suspicious activity or potential AML violations." But the Firm's AML procedures still failed to identify and provide adequate written guidance on detecting and investigating potentially suspicious trading activities by customers in their accounts.

Between February 2005 and April 2008, except for the Firm's application of the Analytics Volume Report, Scottrade's AML policies, procedures, and internal controls were not designed to detect and cause the reporting of suspicious trading activity, unless such activity was accompanied by suspicious money movement. As a result, the Firm's AML policies, procedures, and internal controls were inadequate to achieve compliance with the Bank Secrecy Act and the

implementing regulations thereunder because they were not reasonably designed to detect and cause the reporting of suspicious securities transactions.

### **Conclusion**

By virtue of the above, during the review period, Scottrade violated NASD Conduct Rules 3011 and 2110 and MSRB Rule G-41 by failing to establish and implement policies and procedures that could reasonably be expected to detect and cause the reporting of transactions required under 31 U.S.C. 5318(g) and the implementing regulations thereunder; and by failing to establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act and the implementing regulations thereunder.

- B. Respondent also consents to the imposition, at a maximum, of the following sanctions:
1. a censure;
  2. a fine of \$600,000; and
  3. an undertaking that the Firm's Chief Compliance Officer shall certify within 60 days of the effective date of this AWC that the Firm is in compliance with FINRA Rule 3011(a) and (b) and MSRB Rule G-41 by establishing and implementing AML policies, procedures, and internal controls with respect to its monitoring for suspicious transactions that are reasonably designed to achieve compliance with the requirements of the Bank Secrecy Act and the Treasury's implementing regulations.

The sanctions imposed herein shall be effective on a date set by FINRA staff.

### **II.**

#### **WAIVER OF PROCEDURAL RIGHTS**

Respondent specifically and voluntarily waives the following rights granted under FINRA's Code of Procedure:

- A. To have a Formal Complaint issued specifying the allegations against it;
- B. To be notified of the Formal Complaint and have the opportunity to answer the allegations in writing;
- C. To defend against the allegations in a disciplinary hearing before a hearing panel, to have a written record of the hearing made and to have a written decision issued; and
- D. To appeal any such decision to the National Adjudicatory Council ("NAC") and then to the U.S. Securities and Exchange Commission and a U.S. Court of Appeals.

Further, Respondent specifically and voluntarily waives any right to claim bias or prejudgment of the General Counsel, the NAC, or any member of the NAC, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including acceptance or rejection of this AWC.

Respondent further specifically and voluntarily waives any right to claim that a person violated the *ex parte* prohibitions of FINRA Rule 9143 or the separation of functions prohibitions of FINRA Rule 9144, in connection with such person's or body's participation in discussions regarding the terms and conditions of this AWC, or other consideration of this AWC, including its acceptance or rejection.

### III.

#### OTHER MATTERS

Respondent understands that:

- A. Submission of this AWC is voluntary and will not resolve this matter unless and until it has been reviewed and accepted by the NAC, a Review Subcommittee of the NAC, or the Office of Disciplinary Affairs ("ODA"), pursuant to FINRA Rule 9216;
- B. If this AWC is not accepted, its submission will not be used as evidence to prove any of the allegations against the Firm; and
- C. If accepted:
  - 1. this AWC will become part of Respondent's permanent disciplinary record and may be considered in any future actions brought by FINRA or any other regulator against it;
  - 2. this AWC will be made available through FINRA's public disclosure program in response to public inquiries about the Firm's disciplinary record;
  - 3. FINRA may make a public announcement concerning this agreement and the subject matter thereof in accordance with FINRA Rule 8313; and
  - 4. Respondent may not take any action or make or permit to be made any public statement, including in regulatory filings or otherwise, denying, directly or indirectly, any finding in this AWC or create the impression that the AWC is without factual basis. Respondent may not take any position in any proceeding brought by or on behalf of FINRA, or to which FINRA is a party, that is inconsistent with any part of this AWC. Nothing in this provision affects Respondent's right to take legal or factual positions in litigation or other legal proceedings in which FINRA is not a party.

- D. Respondent may attach a Corrective Action Statement to this AWC that is a statement of demonstrable corrective steps taken to prevent future misconduct. Respondent understands that it may not deny the charges or make any statement that is inconsistent with the AWC in this Statement. This Statement does not constitute factual or legal findings by FINRA, nor does it reflect the views of FINRA or its staff.

Respondent certifies that it has read and understands all of the provisions of this AWC and has been given a full opportunity to ask questions about it; that it has agreed to its provisions voluntarily; and that no offer, threat, inducement, or promise of any kind, other than the terms set forth herein and the prospect of avoiding the issuance of a Complaint, has been made to induce the Firm to submit it.

Date

9/4/09

Respondent Scottrade Inc.

By: A.C. SMALL, GENERAL COUNSEL  
[Name and title]

Reviewed by:

Betty Santangelo

Betty Santangelo  
Counsel For Respondent  
Schulte Roth & Zabel, LLP  
919 Third Avenue  
New York, New York 10022

Accepted by FINRA:

10/26/09  
Date

Signed on behalf of the  
Director of ODA, by delegated  
authority



Samuel L. Israel  
Associate Vice President and Chief  
Counsel  
FINRA Department of Enforcement  
1801 K Street, N.W., Suite 800  
Washington, D.C. 20006-1334  
(t) 202-974-2868  
(f) 202-721-8316

## Resources (/resources)

Alerts/Advisories/Notices/Bulletins/Fact Sheets (/resources/advisoriesbulletinsfact-sheets)

COVID-19 Information (/coronavirus)

Filing Information (/resources/filing-information)

Financial Institutions (/resources/financial-institutions)

FinCEN Exchange (/resources/financial-crime-enforcement-network-exchange)

Innovation (/resources/fincens-innovation-initiative)

International (/resources/international-programs)

Law Enforcement (/resources/law-enforcement-overview)

SAR Stats (/reports/sar-stats)

## Statutes and Regulations (/fincens-legal-authorities)

**Bank Secrecy Act (/resources/statutes-and-regulations/bank-secrecy-act)**

**[BSA Timeline \(/resources/statutes-and-regulations/bank-secrecy-act/bsa-timeline\)](#)**

Chapter X (/resources/statutes-regulations/chapter-x)

Federal Register Notices (/resources/statutes-regulations/federal-register-notices)

Administrative Rulings (/resources/statutes-regulations/administrative-rulings)

Guidance (/resources/statutes-regulations/guidance)

USA PATRIOT Act (/resources/statutes-regulations/usa-patriot-act)

311 and 9714 Special Measures (/resources/statutes-and-regulations/311-and-9714-special-measures)

CDD Final Rule (/resources/statutes-and-regulations/cdd-final-rule)



Suspicious Activity Report (SAR) Advisory  
Key Terms (/resources/suspicious-activity-report-sar-advisory-key-terms)

Reports (/resources/financial-trend-analyses)

# BSA Timeline

		
<b>1970</b>	Large currency deposits of illicit profits	<i>Bank Secrecy Act (BSA) enacted</i>
<b>1974</b>	Constitutionality of Bank Secrecy Act questioned	<i>U.S. Supreme Court holds BSA to be constitutional</i>
<b>1986</b>	Law Enforcement looks for new weapons to combat drug trafficking	<i>Enact Money Laundering Control Act</i>
<b>1990</b>	Insufficient intelligence analysis and resources to support financial investigations	<i>Create Financial Crimes Enforcement Network (FinCEN)</i>
<b>1992</b>	Law enforcement needs more information on suspicious transactions to support financial investigations	<i>Enact Annunzio-Wylie Money Laundering Suppression Act - Suspicious activity reporting required</i>
<b>1994</b>	Law enforcement focuses on criminal abuse of MSBs CTR exemption process is a burden for financial community	<i>Enact Money Laundering Suppression Act - MSB registration CTR filing required</i>
<b>1994</b>	Improve cooperation and coordination between regulatory, financial and law enforcement communities	<i>Merge Treasury's Office of Financial Enforcement with FinCEN - FinCEN's Mission expanded to include regulatory authority</i>

# Timeline

1970 - Present

1998	Improve coordination of federal, state and local efforts and resources to combat financial crimes	Enact Money Laundering & Financial Crimes Strategy Act - National Money Laundering strategy established - HIFCA system created
2000	Law enforcement needs more information on money transmitters, and issuers, sellers and redeemers of money	MSBs required to file suspicious Activity Reports (SARs)
2001	Terrorists attack the World Trade Center & Pentagon; President announces ( <a href="http://georgewbush-whitehouse.archives.gov/news/releases/2001/11/20011107-4.html">http://georgewbush-whitehouse.archives.gov/news/releases/2001/11/20011107-4.html</a> ) Financial War on Terror at FinCEN	Enact PATRIOT Act - Information Sharing - Registration requirements for underground money transmitters
2002	Institutions are front line against money laundering and terrorist financing	Most financial institutions receive a new or amended AML Program requirement
2002	Law enforcement needs more information on casinos	Casinos required to file SARs
2002	Importance of information sharing recognized	Sharing between institutions is protected, and between institutions and government is required
2002	Foreign shell banks recognized as threat	Termination of accounts for shell banks and certification by foreign correspondents required
2002	Financial institutions seek to expedite reporting process, reduce costs in complying with BSA requirements	PATRIOT Act Communications System (PACS) launched - Financial institutions can file BSA reports electronically
2002	PATRIOT Act expands regulatory definition of "financial institution"	Brokers and dealers in securities must file SARs
2003	Need to protect more MSBs from financial crimes	Currency Dealers and Exchangers required to file SARs

# Timeline

1970 - Present

2003	Identification requirement strengthened	<i>Customer Identification Programs required for most financial institutions</i>
2003	Need to protect casinos from money launderers	<i>Casinos and card clubs required to file SARs - includes those operated on tribal lands</i>
2003	FinCEN expands regulatory definition of "financial institution"	<i>Futures commission merchants, introducing brokers in commodities required to report suspicious transactions</i>
2004	U.S. financial system needs additional protection from risks of financial crime posed by foreign agents	<i>MSBs receive guidance for dealing with foreign agents and foreign counterparts</i>
2005	Certain account services need greater scrutiny	<i>Due diligence requirements for private banking and foreign correspondent</i>
2005	Improve management of BSA data, from filing and storage to retrieval and analysis	<i>PACS renamed as BSA E-Filing - 25% of BSA filings and 40% of SARs are e-filed as of March 2005</i>
2005	Improve collaboration and information sharing between federal and state agencies	<i>FinCEN, 29 states sign Memoranda of Understanding (MOU) -established information sharing agreements</i>
2005	Jewelry industry needs protection against financial crime	<i>Jewelers, dealers in precious metals and stones required to establish anti-money laundering (AML) programs</i>
2005	Increased international effort to combat money laundering, terrorist financing	<i>Egmont Group of financial intelligence units exceeds 100-member mark</i>

# Timeline

*1970 - Present*

<b>2005</b>	Need to ensure consistent application of BSA to all banking organizations	<i>Federal banking agencies release BSA/AML Examination Manual</i>
<b>2005</b>	Need to protect insurance industry from financial crimes	<i>Certain insurance companies required to establish AML programs, file SARs</i>
<b>2006</b>	Need to protect mutual funds from financial crimes	<i>Mutual funds required to file SARs</i>
<b>2007</b>	Certain account services need greater scrutiny	<i>Enhanced due diligence is required for certain foreign correspondent banks</i>
<b>2009</b>	Need to simplify requirements for depository institutions to exempt their eligible customers from currency transaction reporting	<i>Final Rule on CTR Exemptions takes effect (Jan. 5, 2009)</i>
<b>2011</b>	Need to enhance efficiency and effectiveness	<i>Transfer of FinCEN's regulations to 31 CFR Chapter X</i>
<b>2011</b>	MSB rules amended to establish a more comprehensive regulatory approach for prepaid access	<i>FinCEN issues prepaid access Final Rule (Effective Date: September 27, 2011; Compliance Date: January 29, 2012)</i>
<b>2012</b>	Need to combat fraud in the non-bank residential mortgage sector	<i>Final Rule defines non-bank residential mortgage lenders and originators (RMLOs) as loan or finance companies. RMLOs required to establish AML programs and file SARs (Effective Date: April 16, 2012; Compliance Date: August 13, 2012)</i>
<b>2014</b>	Law enforcement and regulators need more complete and timely information on suspected mortgage fraud and money laundering	<i>Housing GSEs required to develop AML programs and file SARs (Effective Date: April 28, 2014; Compliance Date: August 25, 2014)</i>

# Timeline

1970 - Present

2016

Need to clarify and strengthen customer due diligence requirements for banks; brokers or dealers in securities; mutual funds; and futures commission merchants and introducing brokers in commodities

*Final Rule contains explicit customer due diligence requirements and includes a new requirement to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions (Effective Date: July 11, 2016; Compliance Date: May 11, 2018)*



[Home \(/\)](#)

[Resources \(/resources\)](#)

[Contact \(/contact\)](#)

[About \(/what-we-do\)](#)

[Careers \(/cutting-edge-opportunities\)](#)

[Newsroom \(/news-room\)](#)

[Contract Opportunities \(/about/contract-opportunities\)](#)

[Get News Updates \(https://service.govdelivery.com/accounts/USFINCEN/subscriber/new\)](https://service.govdelivery.com/accounts/USFINCEN/subscriber/new)

## Languages

[USA.gov \(https://www.USA.gov\)](https://www.USA.gov) | [Regulations.gov \(https://www.Regulations.gov\)](https://www.Regulations.gov) | [Treasury.gov \(https://www.treasury.gov\)](https://www.treasury.gov) | [IRS.gov \(https://www.IRS.gov\)](https://www.IRS.gov) | [Freedom of Information Act \(FOIA\) \(/freedom-information-act-foia-and-guide-accessing-fincen-information\)](#) | [NO FEAR Act \(https://home.treasury.gov/footer/no-fear-act\)](https://home.treasury.gov/footer/no-fear-act) | [Vote.gov \(https://vote.gov/\)](https://vote.gov/) | [Accessibility \(/accessibility\)](#) | [EEO & Diversity Policy \(/equal-employment-opportunity-and-diversity-policy\)](#) | [Privacy Policy \(/privacy-security\)](#) | [Public Posting Notice of Finding of Discrimination \(https://home.treasury.gov/footer/no-fear-act\)](https://home.treasury.gov/footer/no-fear-act) | [Security and Vulnerability Disclosure Policies \(VDP\) \(/security-and-vulnerability-disclosure-policies\)](#)



# FinCEN ADVISORY

FIN-2022-A002

June 15, 2022

## Advisory on Elder Financial Exploitation

***Amid rampant fraud and abuse targeting older adults, FinCEN urges financial institutions to detect, prevent, and report suspicious financial transactions.***

**Elder financial exploitation (EFE)** is defined as the illegal or improper use of an older adult's funds, property, or assets.<sup>1</sup>

### **SAR Filing Request:**

FinCEN requests that financial institutions reference the advisory by including "**EFE FIN-2022-A002**" in SAR field 2 ("Filing Institution Note to FinCEN"), and mark the check box for elder financial exploitation.

## Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to alert financial institutions to the rising trend of EFE targeting older adults<sup>2</sup> and to highlight new EFE typologies and red flags since FinCEN issued the first EFE Advisory in 2011.<sup>3</sup> FinCEN is also issuing this advisory in support of World Elder Abuse Awareness Day, which has been commemorated on June 15 every year since 2006 and provides an opportunity for communities around the world to promote a better understanding of abuse and neglect of older adults by raising awareness of the related cultural, social, economic, and demographic factors.<sup>4</sup>

According to the U.S. Department of Justice, elder abuse, which includes EFE among other forms of abuse, affects at least 10 percent of older adults each year in the United States,<sup>5</sup> with millions of older adults losing more than \$3 billion to financial fraud annually as of 2019.<sup>6</sup> Despite the

1. EFE is one type of elder abuse, which includes physical, emotional, and financial abuse. Elder abuse and EFE definitions vary statutorily by state. For more information on the definition of EFE, see Consumer Financial Protection Bureau (CFPB) and FinCEN, "[Memorandum on Financial Institution and Law Enforcement Efforts to Combat Elder Financial Exploitation](#)," (Memorandum on EFE) (August 30, 2017); see also, U.S. Department of Justice (DOJ) webpage, [Elder Abuse and Elder Financial Exploitation Statutes](#).
2. For purposes of this advisory and consistent with other U.S. government agencies' use of the term, an older adult is considered an individual 60 years of age or older. See Federal Trade Commission (FTC) Report, "[Protecting Older Consumers, 2020-2021](#)," (Older Consumers Report) (October 18, 2021), at p. 1.
3. See FinCEN, "[Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation](#)," (2011 Advisory) (February 22, 2011).
4. For more information about World Elder Abuse Awareness Day, see Administration for Community Living (ACL), [World Elder Abuse Awareness Day](#).
5. For more information on EFE, see DOJ, [About Elder Abuse](#).
6. See Internet Crime Complaint Center (IC3), "[Perpetrators Use Various Methods to Deceive and Defraud Elderly Victims For Financial Gain](#)," (September 19, 2019). Fraud (of all types) is the largest proceeds-generating offense in the United States and is one of the [FinCEN June 2021 anti-money-laundering/counter-financing-of-terrorism \(AML/CFT\) National Priorities](#).



fact that EFE is the most common form of elder abuse, the majority of incidents go unidentified and unreported as victims may choose not to come forward out of fear, embarrassment, or lack of resources.<sup>7</sup> Older adults are targets for financial exploitation due to their income and accumulated life-long savings, in addition to the possibility that they may face declining cognitive or physical abilities, isolation from family and friends, lack of familiarity or comfort with technology, and reliance on others for their physical well-being, financial management, and social interaction.<sup>8</sup> The COVID-19 pandemic exacerbated these vulnerabilities for many older adults.<sup>9</sup> In 2020, over 62,000 suspicious activity reports (SARs) related to EFE were filed, totaling what the Consumer Financial Protection Bureau (CFPB) estimates to be \$3.4 billion in suspicious transactions, an increase from \$2.6 billion in 2019. This is the largest year-to-year increase since 2013.<sup>10</sup> This trend has continued with over 72,000 SARs related to EFE filed in 2021 and, according to the Federal Trade Commission (FTC), older adults now account for 35 percent of the victims associated with filed fraud reports in cases when a consumer provided an age.<sup>11</sup>

The U.S. government has multiple initiatives in place to counter perpetrators and facilitators of EFE.<sup>12</sup> In support of this whole-of-government approach, FinCEN collaborates with law enforcement, regulatory agencies, and financial institutions to ensure that SARs appropriately identify and report suspicious activity potentially indicative of EFE. Financial institutions are uniquely situated to detect possible financial exploitation through their relationships with older customers. They therefore play a critical role in helping to identify, prevent, and report EFE to law enforcement and their state-based Adult Protective Services,<sup>13</sup> and any other appropriate first

7. See CFPB and FinCEN, Memorandum on EFE, *supra* Note 1. See also, FTC Older Consumers Report, *supra* Note 2.

8. See CFPB and FinCEN, Memorandum on EFE, *supra* Note 1.

9. See DOJ Office of Public Affairs (OPA), [“Associate Attorney General Vanita Gupta Delivers Remarks at the Elder Justice Coordinating Council Meeting,”](#) (December 7, 2021); see also, DOJ OPA, [“Statement of Attorney General Merrick B. Garland on World Elder Abuse Awareness Day,”](#) (June 15, 2021); and [“Associate Deputy Attorney General Paul R. Perkins Delivers Remarks at the ABA/ABA Financial Crimes Enforcement Conference,”](#) (December 9, 2020).

10. See CFPB, [“Suspicious Activity Reports on Elder Financial Exploitation.”](#)

11. See FinCEN, [SAR Stats](#); and FTC, [“Consumer Sentinel Network: Data Book 2021,”](#) (February 2022), at p. 13.

12. See DOJ’s [Elder Justice Initiative](#), [Transnational Elder Fraud Strike Force](#), and [Money Mule Initiative](#). For U.S. government efforts to address romance scams, see [Dating or Defrauding: A National Awareness Campaign](#). Additionally, passed in 2010, the Elder Justice Act was the first comprehensive legislation to address the abuse, neglect, and exploitation of older adults at the federal level. The law authorized a variety of programs and initiatives to better coordinate federal responses to elder abuse, promote elder justice research and innovation, support Adult Protective Services systems, and provide additional protections for residents of long-term care facilities. Further, the Elder Justice Act established the Elder Justice Coordinating Committee to coordinate activities related to elder abuse, neglect, and exploitation across the federal government. For more information about the Elder Justice Act and the associated Committee, visit the [Administration for Community Living, Elder Justice Act](#). See also, the [National Center on Elder Abuse \(NCEA\)](#).

13. According to the National Adult Protective Services Association (NAPSA), “Adult Protective Services (APS) programs promote the safety, independence, and quality-of-life for vulnerable adults who are, or are in danger of, being abused, neglected by self or others, or financially exploited, and who are unable to protect themselves. APS is a social service program authorized by law in every state to receive and investigate reports of elder or vulnerable adult maltreatment and to intervene to protect the victims to the extent possible.” See NCEA, NAPSA, and Keck School of Medicine of USC, [“Fact Sheet: Adult Protective Services, What You Must Know,”](#) and NCEA, [Adult Protective Services](#); and [How APS Works](#).

responder as well as assisting older customers who fall victim to financial exploitation.<sup>14</sup> The information contained in this advisory is derived from FinCEN's analysis of Bank Secrecy Act (BSA) data, open source reporting, and law enforcement partners.

## Trends and Typologies of EFE and Associated Payments

EFE schemes generally involve either theft or scams.<sup>15</sup> Perpetrators of elder theft are often known and trusted persons of older adults, while scams, which can disproportionately affect older adults, frequently involve fraudsters, often located outside of the United States, with no known relationship to their victims.<sup>16</sup> Regardless of the relationship, these criminals can place older adults in financially, emotionally, and physically compromising situations, and the resulting loss of income and life-long earnings can be devastating to the financial security, dignity, and quality of life of the victims.<sup>17</sup>

### Elder Theft

*Schemes involving the theft of an older adult's assets, funds, or income by a trusted person.*

### Elder Scams

*Scams involving the transfer of money to a stranger or imposter for a promised benefit or good that the older adult did not receive.*

Unfortunately, perpetrators of EFE schemes often do not stop after first exploiting their victims. In both elder theft and scams, older adults are often re-victimized and subject to potentially further financial loss, isolation, and emotional or physical abuse long after the initial exploitation due to the significant illicit gains at stake.<sup>18</sup> Scammers may also sell victims' personally identifiable information (PII) on the black market to other criminals who continue to target the victims using new and emerging scam typologies.<sup>19</sup>

### Elder Theft

Perpetrators of elder theft are often family members and non-family caregivers who abuse their relationship and position of trust. As identified by FinCEN in 2019 in its analysis of a statistically

14. Reporting EFE to APS, law enforcement, or other authorities is an opportunity to strengthen prevention and response. See CFPB, "[Reporting of Suspected Elder Financial Exploitation by Financial Institutions](#)," (July 17, 2019); "[Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends](#)," (February 2019); CFPB and FinCEN, Memorandum on EFE, *supra* Note 1; and Federal Reserve, CFTC, CFPB, FDIC, FTC, NCUA, OCC, and SEC, "[Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults](#)," (September 24, 2013).
15. See FinCEN Financial Trend Analysis (FTA), "[Elders Face Increased Financial Threat from Domestic and Foreign Actors](#)," (December 2019), at p. 4.
16. *Id.*
17. See CFPB and FinCEN, Memorandum on EFE, *supra* Note 1.
18. For additional information on re-victimization in EFE schemes, see FINRA Investor Education Foundation (FINRA Foundation), American Association of Retired Persons (AARP), and Heart+Mind Strategies, "[Addressing the Challenge of Chronic Fraud Victimization](#)," (March 2021).
19. See DOJ, "[List Brokerage Firm Pleads Guilty to Facilitating Elder Fraud Schemes](#)," (September 28, 2020).



significant, random sampling of SAR narratives, a family member was involved in the theft of assets from older adults in 46 percent of elder theft cases reported between 2013 and 2019.<sup>20</sup> Trusted persons who commit elder theft can also include familiar associates and acquaintances such as neighbors, friends, financial services providers, other business associates, or those in routine close proximity to the victims.

Instances of elder theft often follow a similar methodology in which trusted persons may use deception, intimidation, and coercion against older adults in order to access, control, and misuse their finances. Criminals frequently exploit victims' reliance on support and services and will take advantage of any cognitive and physical disabilities,<sup>21</sup> or environmental factors such as social isolation, to establish control over the victims' accounts, assets, or identity.<sup>22</sup> This can take many forms, including the exploitation of legal guardianships<sup>23</sup> and power of attorney arrangements,<sup>24</sup> or the use of fraudulent investments such as Ponzi schemes<sup>25</sup> to defraud older adults of their income and retirement savings. These relationships enable trusted persons to repeatedly abuse the victims by liquidating savings and retirement accounts, stealing Social Security benefit checks and other income, transferring property and other assets, or maxing out credit cards in the name of the victims until most of their assets are stolen.<sup>26</sup>

## Case Study on Elder Theft

### Housekeeper and Co-Conspirators Exploit Dementia-afflicted Older Adult

A woman in Charlotte, North Carolina was convicted and sentenced to 97 months in prison and two years of supervised release for conspiracy to commit wire fraud and money laundering conspiracy. Donna Graves, who was the ringleader of the criminal conspiracy, conspired to engage in a scheme to defraud a victim identified in court documents as "K.T." The victim was an elderly widow who lived alone and suffered from dementia and other physical and mental challenges. During the relevant time period, Graves and her co-conspirators (Gerald Maxwell Harrison and Elizabeth Robin Williams) exploited K.T.'s vulnerabilities and defrauded the victim through a web of forged documents, lies, and deceptions. According to evidence presented at Graves' trial, beginning in 2014, Graves and Williams provided housekeeping services for the victim through a business owned and operated by Graves. Over the course of the scheme, the co-conspirators isolated the victim from her friends and family, induced

20. See FinCEN FTA, *supra* Note 15, at p. 7.

21. *Id.*

22. See DOJ, "[Associate Deputy Attorney General Paul R. Perkins Delivers Remarks at the ABA/ABA Financial Crimes Enforcement Conference](#)," (December 9, 2020).

23. See DOJ, "[Court-Appointed Pennsylvania Guardian and Virginia Co-Conspirators Indicted for Stealing Over \\$1 Million from Elderly Wards](#)," (June 30, 2021).

24. See DOJ, "[Franklin, Tennessee Couple Charged With Defrauding Elderly Widow of \\$1.7 Million](#)," (May 12, 2021); and "[Former Waterloo Medicaid Provider Sentenced to More than Five Years in Federal Prison for Defrauding Elderly Victim](#)," (June 28, 2021).

25. See DOJ, "[Arizona Man Sentenced for Multimillion-Dollar Nationwide Investment Fraud Scheme](#)," (March 15, 2021).

26. See generally, DOJ, "[Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse](#)," (October 18, 2021).

the victim to give them power and control over her personal affairs, and fabricated a power of attorney purporting to give Graves and Williams control over the victim's financial affairs. Once they gained access and control, Graves, Williams, and Harrison moved the victim out of her residence in Indian Land, South Carolina, first to an apartment in Charlotte, and later to a rental home in Mint Hill, refusing to let the victim's friends and family know where she was living. Over the course of the scheme, Graves and her co-conspirators failed to provide the victim with proper medical care, which greatly diminished the victim's health. Furthermore, once the victim's money was depleted, the co-conspirators abandoned the victim, who was later moved to a nursing home in New York, where she passed away in large part due to the mental and physical deterioration she had suffered in the hands of Graves and her co-conspirators.<sup>27</sup>

### Elder Scams

In elder scams, criminals defraud victims into sending payments and disclosing PII under false pretenses or for a promised benefit or good the victims will never receive. These scammers are often located outside of the United States and have no known previous relationship to the victims.<sup>28</sup> Elder scams often follow a similar methodology in which scammers contact older adults under a fictitious persona via phone call, robocall, text message, email, mail, in-person communication, online dating apps and websites, or social media platforms. In order to appear legitimate and establish trust with older adults, scammers commonly impersonate government officials, law enforcement agencies, technical and customer support representatives, social media connections, or family, friends, and other trusted persons. Perpetrators often create high-pressure situations by appealing to their victims' emotions and taking advantage of their trust or by instilling fear to solicit payments and PII.<sup>29</sup> Scammers often request victims to make payments through wire transfers at money services businesses (MSBs), but are increasingly requesting payments via prepaid access cards, gift cards, money orders, tracked delivery of cash and high-valued personal items through the U.S. Postal Service, ATM deposits, cash pick-up at the victims' houses, and convertible virtual currency (CVC).<sup>30</sup>

Further, elder scams are sometimes facilitated through money mules<sup>31</sup> who transfer or move illicit funds at the direction of the scammers. A victim of an elder scam can also serve as a money mule: the scammer convinces the victim to set up a bank account or limited liability corporation (LLC)

27. See DOJ, "[Charlotte Woman And Her Co-Conspirator Are Sentenced To Prison For Stealing \\$300,000 From An Elderly, Dementia-Afflicted Victim](#)," (May 5, 2021).

28. Nigeria, Jamaica, Ghana, India, the Philippines, and the People's Republic of China are the top foreign-located subject countries in MSB SAR Filings. See FinCEN FTA, *supra* Note 15, at p. 9.

29. See generally, FTC, [Imposter Scams](#).

30. See IC3, "[2021 Elder Fraud Report](#)," (March 2022); "[Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams](#)," (September 16, 2021); "[FBI Warns of a Grandparent Fraud Scheme Using Couriers](#)," (July 29, 2021); FTC, "[New Twist to Grandparent Scam: Mail Cash](#)," (December 3, 2018); and DOJ, "[U.S. Attorney Dena J. King Announces The Successful Forfeiture And Return Of Stolen Cryptocurrency To Elderly Man Victimized By Government Imposter Scam](#)," (March 15, 2022).

31. A money mule is a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another. See IC3, "[Money Mules: A Financial Crisis](#)," (December 3, 2021); and Federal Bureau of Investigation (FBI), [Money Mules](#).

in the victim's own name to receive, withdraw, deposit, or transfer multiple third-party payments from other victimized older adults to accounts controlled by the scammer under the illusion of a "business opportunity." In some circumstances, victims of EFE acting as money mules may be prosecuted for this illegal activity and are liable for repaying the victims. They may also be subject to damaged credit and further victimized through their stolen PII.<sup>32</sup>

## Common Elder Scam Typologies

- **Government imposter scams:** Scammers frequently target older adults by impersonating officials from U.S. government agencies that are often well-known or provide services to older adults, such as the Social Security Administration (SSA),<sup>33</sup> the Department of Health and Human Services/Centers for Medicare and Medicaid Services (HHS/CMS),<sup>34</sup> and the Internal Revenue Service (IRS),<sup>35</sup> among others.<sup>36</sup> The scammers may threaten the individuals with arrest or seizure of their bank accounts for crimes they supposedly committed, such as tax evasion. Scammers may also claim that victims' Social Security numbers are suspended due to suspicious activity and demand PII and payment to resolve the supposed matter with the government.<sup>37</sup>
- **Romance scams:** These scams (also referred to as "online dating," "confidence," or "sweetheart" scams) grew to a record level in 2021 with \$547 million in reported losses.<sup>38</sup> Romance scams involve fraudsters creating a fictitious profile on an online dating app or website to establish a close or romantic relationship with older adults to exploit their confidence and trust.<sup>39</sup> Online scammers may offer to meet in person (though they almost never do) and ask victims to send money for travel expenses, a sudden "hardship" they experience such as medical costs or legal fees, or a supposed investment or business deal. The scammers often solicit payments over an extended period of time and victims may also send PII as the perpetrators gain the trust of the victims. In some cases, romance scam victims are convinced to open bank accounts and LLCs to receive and send funds as money mules so the scammers can launder their ill-gotten gains from third-party scams.<sup>40</sup>

32. See IC3, "[Money Mules: A Financial Crisis](#)," (December 3, 2021); "[Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules](#)," (August 5, 2019); and FBI, [Money Mules](#).

33. See FTC, "[Growing Wave of Social Security Imposters Overtakes IRS Scam](#)," (April 12, 2019); and Social Security Administration (SSA), [Protect Yourself From Social Security Scams](#).

34. See FTC, "[Protect Yourself Against Medicare Scams](#)," (March 15, 2019).

35. See Internal Revenue Service (IRS), "[IRS Reminds Seniors to Remain on Alert to Phone Scams during Tax Season](#)," (March 23, 2017).

36. See FTC, "[Government Imposter Scams Top the List of Reported Frauds](#)," (July 1, 2019).

37. See FTC, "[How To Avoid a Government Impersonator Scam](#)," (May 2021); and IC3, "[FBI Warns of the Impersonation of Law Enforcement and Government Officials](#)," (March 7, 2022).

38. See FTC, "[Reports of romance scams hit record highs in 2021](#)," (February 10, 2022).

39. Romance scams can also be perpetrated by scammers who the older adult first meets in-person. These scammers can use romantic overtones to unduly influence an older adult and gain their trust and loyalty before perpetrating the scam.

40. See FBI, [Romance Scams](#); and IC3, "[Cyber Actors Use Online Dating Sites To Conduct Confidence/Romance Fraud And Recruit Money Mules](#)," (August 5, 2019).

- ***Emergency/person-in-need scams:*** These schemes (also known as “grandparent scams”) involve scammers contacting older adults and impersonating a grandchild, another relative, an attorney, emergency medical personnel, or a law enforcement official to deceive victims into believing that a loved one is in an emergency situation (e.g., a car accident, medical emergency, under arrest, or stranded in a foreign country) and needs money sent immediately to resolve the situation.<sup>41</sup>
- ***Lottery and sweepstakes scams:*** These scams are a type of advance-fee scheme in which scammers, typically located in jurisdictions outside of the United States, impersonate lottery or sweepstakes representatives, and lawyers claiming that the victims have won a lottery, prize, or sweepstakes. Scammers may target older adults regardless of whether the victims have previously played the lottery or entered in a sweepstakes. The scammers instruct the victims to pay for supposed shipping, taxes, or other fees in order to claim their prize or lottery winnings. Victims never receive their prize or lottery winnings and are often re-victimized with additional requests for payments throughout the scheme until they run out of money.<sup>42</sup>
- ***Tech and customer support scams:*** These scammers impersonate well-known companies as tech and customer support representatives to falsely claim that a virus or other malware has compromised the victims’ computers. Scammers may request remote access to diagnose the alleged problem and will typically attempt to solicit payment for fraudulent software products and tech support services. They also often exploit the remote access to install malware and steal PII and credit card numbers to further defraud the victims.<sup>43</sup> After victims make payments, perpetrators often call back and offer refunds to the victims, claiming their tech and customer support services are no longer available. Perpetrators then will claim to send refund money to the victims’ bank accounts but falsely claim that too much money was refunded. The scammers then induce victims to send payments purportedly to reimburse the tech and customer support company for its “over-refund.” Victims can lose hundreds or thousands of dollars to such refund schemes. A recent evolution of the refund scheme involves perpetrators claiming to be online retailers and purporting to offer a refund for unauthorized transactions on the victims’ accounts.<sup>44</sup>

41. See FTC, “[Scammers Use Fake Emergencies to Steal Your Money](#),” (May 2021).

42. See FTC, “[Fake Prize, Sweepstakes, and Lottery Scams](#),” (May 2021); and DOJ, [Senior Scam Alert](#).

43. See CFPB, “[What you should know about tech support scams](#),” (January 12, 2021); FTC, “[How to Spot, Avoid, and Report Tech Support Scams](#),” (February 2019); “[Older Adults Hardest Hit By Tech Support Scams](#),” (March 7, 2019); and IC3, “[Technical and Customer Support Fraud](#),” (March 16, 2022).

44. See DOJ, [Transnational Elder Fraud Strike Force](#); and FTC, “[Amazon tops list of impersonated businesses](#),” (October 20, 2021).

## Case Study of Elder Scams

### India-based Government Imposter Scam

An Indian national was sentenced to 22 years in prison for conspiracy and identity theft in connection with his operation of an overseas robocall scam that defrauded thousands of victims out of more than \$10 million. The victims, many of whom are elderly, continue to endure significant financial hardship from the defendant's vast fraud enterprise. According to court documents, Shehzadkhan Pathan, 40, operated a call center in Ahmedabad, India, from which automated robocalls were made to victims in the United States. After establishing contact with victims through these automated calls, Pathan and other "closers" at his call center would coerce, cajole, and trick victims into sending bulk cash through physical shipments and electronic money transfers. Pathan and his conspirators used a variety of schemes to convince victims to send money, including impersonating law enforcement officers from the Federal Bureau of Investigation and Drug Enforcement Administration and representatives of other government agencies, such as the Social Security Administration, to threaten victims with severe legal and financial consequences. Conspirators also convinced victims to send money as initial installments for falsely promised loans. Pathan is the fourth of six defendants in this case to be sentenced for their role in the conspiracy.<sup>45</sup>

## Behavioral and Financial Red Flags of EFE and Associated Payments

FinCEN has identified behavioral and financial red flags to help financial institutions detect, prevent, and report suspicious activity connected to EFE. These red flags build off of the red flags in FinCEN's 2011 Advisory, all of which remain relevant, and do not reflect all behavioral and financial red flags of EFE.<sup>46</sup> As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a behavior or transaction is suspicious or otherwise indicative of EFE. In line with their risk-based approach to compliance with the BSA, financial institutions are also encouraged to perform additional due diligence where appropriate. Financial institutions should remain alert to any suspicious activity indicating that their customers are perpetrators, facilitators, or victims of EFE.











45. See DOJ, "[Leader of International Robocall Scam Sentenced for Defrauding Over 4,000 U.S. Victims Out of More Than \\$10 Million](#)," (September 16, 2021).



46. See 2011 Advisory, *supra* Note 3. For more information on red flags of EFE, see DOJ, [Red Flags of Elder Abuse](#); and CFPB, "[Recommendations and Report for Financial Institutions on Preventing and Responding to Elder Financial Exploitation](#)," (March, 23, 2016).



### Behavioral Red Flags













Victims of EFE may have limited and irregular contact with others. For some, their only outside contact may involve visiting or communicating with their local financial institution, including at the bank branch, check-cashing counter, or MSB. Therefore, it is critical for customer-facing staff to identify and consider the behavioral red flags when conducting transactions involving their older customers, particularly suspicious behavior that also involves the financial red flags highlighted below. Such information should be incorporated into SAR filings and reported to law enforcement as appropriate. Financial institutions are reminded that behavioral red flags of EFE and the names of staff who witnessed them should be included in the SAR narrative to assist future law enforcement investigations. Behavioral red flags of EFE may include:

-  1 An older customer's account shows sudden and unusual changes in contact information or new connections to emails, phone numbers, or accounts that may originate overseas.
-  2 An older customer with known physical, emotional, and cognitive impairment has unexplainable or unusual account activity.
-  3 An older customer appears distressed, submissive, fearful, anxious to follow others' directions related to their financial accounts, or unable to answer basic questions about account activity.
-  4 An older customer mentions how an online friend or romantic partner is asking them to receive and forward money to one or more individuals on their behalf or open a bank account for a "business opportunity."
-  5 During a transaction, an older customer appears to be taking direction from someone with whom they are speaking on a cell phone, and the older customer seems nervous, leery, or unwilling to hang up.
-  6 An older customer is agitated or frenzied about the need to send money immediately in the face of a purported emergency of a loved one, but the money would be sent to the account of a seemingly unconnected third-party business or individual.
-  7 A caregiver or other individual shows excessive interest in the older customer's finances or assets, does not allow the older customer to speak for himself or herself, or is reluctant to leave the older customer's side during conversations.
-  8 An older customer shows an unusual degree of fear or submissiveness toward a caregiver, or expresses a fear of eviction or nursing home placement if money is not given to a caretaker.
-  9 The financial institution is unable to speak directly with the older customer, despite repeated attempts to contact him or her.
-  10 A new caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of an older customer without proper documentation.

-  11 An older customer's financial management changes suddenly, such as through a change of power of attorney, trust, or estate planning vehicles, to a different family member or a new individual, particularly if such changes appear to be done under undue influence, coercion, or forgery or the customer has diminished cognitive abilities and is unable to agree to or understand the consequences of the new arrangement.
-  12 An older customer lacks knowledge about his or her financial status, or shows a sudden reluctance to discuss financial matters.

### Financial Red Flags

Identification of financial red flags of EFE and the associated payments are critical to detecting, preventing, and reporting suspicious activity potentially indicative of EFE. In addition to the financial red flags set out in DOJ and CFPB notices,<sup>47</sup> financial red flags of EFE may include:

-  13 Dormant accounts with large balances begin to show constant withdrawals.
-  14 An older customer purchases large numbers of gift cards or prepaid access cards.
-  15 An older customer suddenly begins discussing and buying CVC.
-  16 An older customer sends multiple checks or wire transfers with descriptors in the memo line such as "tech support services," "winnings," or "taxes."
-  17 Uncharacteristic, sudden, abnormally frequent, or significant withdrawals of cash or transfers of assets from an older customer's account.
-  18 An older customer receives and transfers money interstate or abroad to recipients with whom they have no in-person relationship, and the explanation seems suspicious or indicative of a scam or money mule scheme.
-  19 Frequent large withdrawals, including daily maximum currency withdrawals from an ATM.
-  20 Sudden or frequent non-sufficient fund activity.
-  21 Uncharacteristic nonpayment for services, which may indicate a loss of funds or of access to funds.
-  22 Debit transactions that are inconsistent for the older customer.
-  23 Uncharacteristic attempts to wire large sums of money.
-  24 Closing of CDs or accounts without regard to penalties.

---

47. *Id.*

## Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

*Suspicious Activity Reporting*  
*Other Relevant BSA Reporting*  
*USA PATRIOT ACT Section 314(b) Information Sharing Authority*  
*Additional Reporting Options*

### Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including EFE.<sup>48</sup> All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.<sup>49</sup>

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.<sup>50</sup> Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.<sup>51</sup> When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML/CFT program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

48. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. All financial institutions with these SAR filing requirements also may file a SAR regardless of the amount involved (if any) or if the transaction is only attempted.

49. See 31 U.S.C. § 5318(g)(3).

50. See 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), and 1030.320(d). 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.

51. *Id.* See also, FinCEN, "[Suspicious Activity Report Supporting Documentation](#)," (June 13, 2007).



## SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information about the activity in the SAR form and narrative. Reporting on how perpetrators of EFE communicate with and target older adults is also useful to law enforcement investigations. **FinCEN requests that financial institutions reference this advisory by including the key term below in SAR field 2 (“Filing Institution Note to FinCEN”)** and the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory.

### “EFE FIN-2022-A002”

Financial institutions that suspect EFE activity should also mark the check box for Elder Financial Exploitation (**SAR Field 38(d)**). FinCEN first added an “Elder Financial Exploitation” checkbox to the SAR Form in 2012 and encourages financial institutions to mark the box when filing an EFE-related SAR. For authorized federal, state, and local law enforcement, the checkbox makes it easier to locate and analyze BSA data related to EFE as detailed above.

Financial institutions should include any and all available information relating to the account and locations involved in the reported activity, identifying information and descriptions of any legal entities or arrangements involved and associated beneficial owners, and any information about related persons or entities involved in the activity. Financial institutions also should provide any and all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.<sup>52</sup>

*Financial institutions wanting to expedite their report of suspicious transactions that may relate to the activity noted in this advisory may call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).<sup>53</sup>*

Filers are reminded, as stated in FinCEN’s Electronic Filing Instructions, that the narrative section of the report is critical to understanding the nature and circumstances of the suspicious activity. The care with which the narrative is completed may determine whether the described activity and its possible criminal nature are clearly understood by investigators. Filers must provide a clear, complete, and concise description of the activity, including what was unusual or irregular that caused suspicion.<sup>54</sup> Filers are also encouraged to determine their obligations to report suspected EFE under state law and report suspected EFE to law enforcement and their state-based Adult Protective Services.

52. See 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), and 1030.320(d)(1)(ii)(A)(2).

53. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local area law enforcement officials.

54. See FinCEN, “[SAR Electronic Filing Instructions](#),” (October 2012).

**FinCEN notes that the tips below are best practices in regard to filing a SAR for suspected EFE and are not regulatory obligations:**

- Provide a statement in the narrative documenting the age and location (county/city) of the target or victim. Provide details about the reporting entity's response, e.g., whether accounts were closed, whether the person was warned that transactions appear to involve fraud, if the person was not permitted to conduct new transactions, etc.
- Provide details about the amounts involved and whether any amounts were refunded to the older customer (as of the submission date of the SAR).
- Reference supporting documentation, including any photos or video footage, in the narrative.
- Cross-report the circumstances leading to the filing of EFE SARs directly to local law enforcement if there is any indication that a) a crime may have been committed and/or b) the older adult may still be at risk for victimization by the suspected abuser. Filers should note that the filing of a SAR is not a substitute for any requirement in a given state to report suspected EFE to law enforcement and Adult Protective Services.
- Take advantage of the law enforcement contact field to indicate if the suspicious activity was also reported to law enforcement or Adult Protective Services, as well as the name and phone number of the contact person.
- Provide direct liaisons or points of contact at the reporting entity related to the SAR so investigators can ask questions and request additional documentation in a timely manner.
- Expedite responses to law enforcement requests for supporting documents.<sup>55</sup>

### **Other Relevant BSA Reporting Requirements**

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements that provide information in connection with the subject of this advisory.<sup>56</sup> These include obligations related to the Currency Transaction Report (CTR),<sup>57</sup> Report of Cash

55. Elder financial exploitation investigations are often complex, time-consuming, and time-sensitive because older victims may be at risk of losing cognitive capacity or passing away before law enforcement has fully investigated the case. Therefore, expedited responses are critical to aiding any investigation.

56. BSA reporting refers to legal requirements that financial institutions and certain businesses and persons report certain financial transactions (such as large-dollar cash transactions), suspicious activity, or other information (such as information on a taxpayer's foreign bank and financial accounts) to FinCEN "that are highly useful in (A) criminal, tax, or regulatory investigations, risk assessments, or proceedings; or (B) intelligence or counterintelligence activities, including analysis, to protect against terrorism;" 31 U.S.C. § 5311(1).

57. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to the reporting financial institution which involves a transaction in currency of more than \$10,000, in aggregate per business day. 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.

Payments Over \$10,000 Received in a Trade or Business (Form 8300),<sup>58</sup> Report of Foreign Bank and Financial Accounts (FBAR),<sup>59</sup> Report of International Transportation of Currency or Monetary Instruments (CMIR),<sup>60</sup> Registration of Money Services Business (RMSB),<sup>61</sup> and Designation of Exempt Person (DOEP).<sup>62</sup> These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

### Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this advisory, FinCEN requests that the filer select **Box 1b** (“suspicious transaction”) and include the key term “EFE FIN-2022-A002” in the “Comments” section of the report.

### Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing EFE, among other illicit activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding activities they suspect may involve possible terrorist financing or money laundering.<sup>63</sup> FinCEN strongly encourages such voluntary information sharing.

### Rapid Response Program

Through the Rapid Response Program (RRP), FinCEN helps victims and their financial institutions recover funds stolen as the result of certain cyber-enabled financial crime schemes, including cyber-enabled fraud against older adults. The RRP is a partnership between FinCEN; U.S. law enforcement (including the FBI, the U.S. Secret Service, Homeland Security Investigations, and the U.S. Postal Inspection Service); and foreign partner agencies that, like FinCEN, are the financial intelligence units (FIUs) of their respective jurisdictions. FinCEN

58. A report filed by any U.S. person engaged in a trade or business on the receipt of more than \$10,000 in currency in one transaction or two or more related transactions involving the trade or business. Such transactions are required to be reported on joint FinCEN/IRS Form 8300 when not otherwise required to be reported under the CTR requirements. 31 CFR §§ 1010.330, 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.
59. A U.S. person that has a financial interest in or signature authority over foreign financial accounts must file an FBAR if the aggregate value of the foreign financial accounts exceeds \$10,000 at any time during the calendar year, as specified in 31 CFR § 1010.350 and FinCEN Form 114.
60. Each person (i.e., an individual or legal entity), as defined in 31 CFR § 1010.100(mm), that transports, ships, or mails more than \$10,000 of currency or other monetary instruments into or out of the United States must file a CMIR. 31 CFR § 1010.340.
61. Report for a business required to register with FinCEN as a money services business, as defined in 31 CFR § 1010.100(ff), or renewing the registration. 31 CFR § 1022.380.
62. Report for banks, as defined in 31 CFR § 1010.100(d), to exempt certain customers from currency transaction reporting in accordance with 31 CFR § 1010.311.
63. For further guidance related to the 314(b) Program, see FinCEN, “[Section 314\(b\) Fact Sheet](#),” (December 20, 2020).

uses its authority to share financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to interdict the fraudulent transactions, freeze funds, and stop and recall payments using their authorities under their own respective legal and regulatory frameworks. A victim of a cyber-enabled crime, or the victim's financial institution, must file a complaint with federal law enforcement to initiate the RRP.

The RRP has been used to confront cyber threats involving over 80 foreign jurisdictions, and has the capacity to reach more than 160 foreign jurisdictions through FIU-to-FIU channels. Through these collaborative efforts, FinCEN has successfully assisted in the recovery of over \$1.1 billion. For more information, please see FinCEN's [Fact Sheet on the Rapid Response Program \(RRP\)](#).

### Other U.S. Government EFE Reporting Options

In addition to filing a SAR, financial institutions should refer their older customers who may be a victim of EFE to the DOJ's [National Elder Fraud Hotline](#) at 833-FRAUD-11 or 833-372-8311 for support, resources, and assistance with reporting suspected fraud to the appropriate government agencies. Filers should immediately report any imminent threat or physical danger to their local FBI office or local law enforcement. FinCEN encourages filers to collaborate with other stakeholders in their communities to enhance responses and engage in professional training opportunities, community education prevention, and awareness activities and initiatives.<sup>64</sup> Filers can find whether there is an existing collaboration on elder fraud prevention and response in their area by contacting Adult Protective Services or their local Area Agency on Aging.<sup>65</sup>

### For Further Information

Questions regarding the contents of this advisory should be addressed to the FinCEN Resource Center at [frc@fincen.gov](mailto:frc@fincen.gov).

**The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.**

64. See CFPB, [Elder Networks](#). This webpage provides additional information about collaboration in communities to prevent and respond to elder financial exploitation.

65. See U.S. Administration on Aging, [Eldercare Locator](#). The website also provides a list of public services available to older adults.



Newsroom > Speeches > Mary L. Schapiro

**Remarks by Mary L. Schapiro  
Vice Chairman, NASD President, Regulatory Policy and Oversight**

**SIA Compliance & Legal Conference  
JW Marriott Desert Ridge  
Phoenix, AZ  
March 22, 2004 (Final)**

Good morning and thank you so much for the opportunity to join you this morning. Of all the invitations I receive, speaking before the SIA Compliance and Legal Division annual conference ranks as among the most important. It is NASD's opportunity to address the industry's compliance and legal professionals *en masse* and that is never a moment I wish to waste.

You all have, to my way of thinking, the hardest and most important jobs in the financial services industry. While we continue to struggle through very difficult times, I shudder to think of where we might be if dedicated and hardworking compliance professionals were not a part of this industry. I hope you will take my comments this morning in that light and with the understanding that I know how hard you work to do what is right.

Those of you who know me or have heard me speak before know I can be pretty straightforward and the current state of markets and investor confidence are very serious topics. So I apologize at the outset if I leave you a bit troubled when I am done. But on the bright side, the matters we will discuss today bode well for the need to keep all of you—indeed *more* of you—fully employed, and productively occupied.

I think it is fair to say that these are days of intense scrutiny for the financial services industry and that these days are here to stay. More about that in a minute. Yes, the market has been headed determinedly in the right direction, investors have continued to pour money into funds, the IPO market is showing robust signs of life—but from where I sit, most of the news is not quite so good.

I have been a regulator for virtually all of my professional life—more than 20 years. And I have been genuinely saddened, and more than a little discouraged, by the drift in professional conduct in our industry and what I see as refusal to deal systemically with the root causes of the problems, and to put forth the effort to lay the foundation necessary for re-establishing trust with the investing public.

As someone who cares deeply about this industry, and understands what it means for millions of Americans, I've been focused on what needs to happen to lay that foundation and to begin to re-earn the public's confidence.

In fact, it was another time and another scandal that actually prompted me to become a regulator in the first place.

When I was getting ready to graduate from law school, on a date that it serves no purpose to mention, the Hunt Brothers of Texas were making front-page news because of their efforts to corner the silver market. Working with others, they managed to buy about half the world's deliverable silver supply. (As the daughter of

an antiques dealer, I despair to think of all of the magnificent sterling candelabra that were melted down for sale....) But as you all know, the Hunt's ultimately failed at their market manipulation, declared personal bankruptcy and a New York jury found them guilty of conspiring to manipulate the price of silver.

It fascinated me that the Hunt's thought they could get away with this fantastic scheme, and it led me to apply for a job with the Commodity Futures Trading Commission, the federal agency that regulates commodity markets. That spring I was offered several jobs: one with the CFTC and others, paying more than twice as much, with law firms. Much to the initial dismay of my father, I joined the CFTC. And, while I could not have imagined it at the time, a life-long interest and career as a market regulator was born.

From the CFTC to the SEC, back to the CFTC and finally to NASD, I have moved between markets and organizations, but always as a regulator and occasionally in response to the kind of scandals that piqued my interest in the Hunt Brothers nearly 25 years ago.

I tell you this story not because it is particularly interesting, but because it is partly this background that leaves me so surprised and so saddened today, and so determined to bring about the changes necessary to rebuild market integrity.

This should be a good time for the industry, with markets rebounding and investors taking another look. Instead, the news continues to be dominated by new scandals and tales of individuals and firms that appear to have forgotten the investor interest altogether.

What else can one think, when just last week *The New York Times* reported allegations that three major bank/broker-dealers underwrote and sold to the public, billions of dollars of WorldCom debt at a time when their internal credit analysts had decided that WorldCom presented an untenable credit risk?

I consider myself pretty seasoned and hard to surprise and yet scenarios like this leave me shaking my head. I don't need to tell you that the financial impact of the year 2000 market break and its aftermath resulted in losses of capitalization that were depression-era in magnitude. Yet, I believe those financial blows pale in comparison to the regulatory fallout and the industry tremors from laying bare the scope of investor protection compromises by many financial services institutions.

Indeed, recent problems have been so serious and so pervasive that they have informed the thinking of the popular culture. When Martha Stewart was found guilty, one juror remarked upon the verdict being a "victory for the little guy" an apparent reference to the stock trading losses of the masses while insiders became increasingly rich. What's interesting is that no charge that reached the jury dealt with any allegation of trading violations or securities fraud. To me, the comment reflects that average investors don't think they had a fair shot and that their anger still runs deep. That is a sad state of affairs for this industry specifically and I believe it presents a general threat to one of our nation's major strengths: a vibrant capital market structure with a point of entry through the many firms we at NASD regulate.

It has become a standard practice for regulators to recite the litany of scandals of the past three years but I will spare you-I know that you know them well and appreciate the important lessons they teach us. And my greatest hope is that this learning has transformed the thinking of the industry in a lasting manner. I must however admit to a concern that, deep down, many on the business side cling to a belief that "this too shall pass," that at some point we will return to the normalcy of lessened regulatory scrutiny and demand, and that some sense of "business as usual" will be regained.

Such thinking, if it does exist, misperceives the lasting effect of recent events. A tipping point has occurred and this industry will, for the foreseeable future, face increased obligations and heightened scrutiny of regulators. There is no reason to pretend that this change is not permanent and dangerous consequences lie

if we fail to recognize this and act accordingly.

Many of you know of the very tangible fallout from recent corporate and market scandals-the enactment of Sarbanes-Oxley, which has had a galvanizing impact on corporate boards and audit committees, the daily parade in the headlines of SEC and NASD enforcement actions and criminal cases for tainted research, market timing, late trading, illegal sales contests, promotion of unsuitable products and on and on, the activism of State Attorneys General, and the vast array of new rules and regulations-NASD alone has filed 95 new rules with the SEC in the last 2 years.

There has also been a less tangible, but nonetheless transforming impact of these scandals on the relationship of regulator to the regulated. If the bond of trust between investors and the industry has been significantly damaged, and it surely has, then in equal measure there has been damage to the bond of trust between regulators and the industry. This is a serious problem for all regulators, but most especially for NASD, as the largest private sector regulator in the world with a budget of half a billion dollars, our work is a combination of enforcement and the encouragement of self-compliance. If we at NASD fail in our regulatory mission, then self-regulation itself will fail and it will vanish. I have a sense that some in this room may not be driven to tears at that prospect.

Yes, we have burdened your regulatory load significantly over the years and inevitably more is to come. And, it is true that NASD often is not aligned with what the industry perceives as its self interest; nevertheless I believe that the ultimate self interest, indeed the survival of the industry, lies in the promotion of balanced and vigorous self-regulation. Let's review the role of self-regulation for just a moment.

NASD has significant independent authority that at first glance looks a lot like the SEC's. We bring enforcement cases-in fact, more of them every year than the SEC, and all other SROs combined-collecting many millions of dollars in fines and removing, through our enforcement efforts, more than 800 brokers a year from the business. We engage in rulemaking that covers the full range of activity within brokerage firms and promotes integrity and information transparency in markets. We also have authority to define our budget and collect it from the industry, something we do with care but for which we have complete authority nonetheless.

But we are not the SEC and one of our greatest strengths lies in our access to industry expertise.

Ultimately, this industry flourishes best on a promise of fidelity between the interests of the broker and the client. And the realization of that promise is best promoted by ethical standards that are the cardinal principles of self-regulation.

OK, I have described self-regulation, but what is it really? This is not just a rhetorical question and I pose it because I think its role is misperceived even within this room. Self-regulation is not regulation by proxy or referendum of the regulated firms. It is not regulation-light. We are not a trade association and we are not a club. I believe self-regulation is best described as regulation informed and illuminated, but not dictated, by interaction with the industry. Self-regulation is a privilege to be earned and to be cherished.

The benefit to the industry is that self-regulation attempts to incorporate the reality of market and industry practice and operations in rulemaking.

The benefit to investors is that our consultation with brokerage firms should ideally give us a better picture of the risks investors face and the protections they need. We are professional regulators, yet we and the regulatory process itself, benefit greatly from the input and active participation of hundreds of industry contributors. The value of SRO participation in the regulatory process is in realizing targeted responses to



problems in industry practice and conduct. We don't just find a problem, make a rule and ignore operational capacities and market impact.

Even though self-regulation does not operate at the pleasure of regulated firms, this does not mean it can operate effectively in an environment in which it is divorced from firms. I said a moment ago that self-regulation is regulation informed and illuminated by the views of the industry. Unfortunately, however, when we see questionable practices, as widespread as those in the mutual fund operational and sales areas, we must question the value of input received from the industry. Anyone looking objectively at the recent and continuing reports would question whether even the basic and most fundamental provisions of the law and commercial honor are being observed within some firms and be left with real doubts about whether they are putting the interests of their clients above all others.

If we cannot assume basic compliance with the rules, what might that mean for self-regulation and for how the industry functions?

Here's one hypothetical. Today we have 600 examiners at the NASD, responsible for inspecting brokerage operations. Our approach to routine examinations, which are in addition to those we do "for cause," is to examine firms on a risk-based cycle—the most concerning each year, all the others every two or four years, resulting in about 2,600 routine exams a year. If instead we felt the need to inspect annually all 5,400 brokerage firms for compliance with every NASD and SEC rule, rather than approaching our task based on a risk assessment, we will need thousands—not hundreds—more examiners, in essence taking up permanent residence inside each firm. We can all recognize that the cost and disruption to business from such an approach would be immense.

We simply must be able to rely on the existence of a basic level of compliance within every firm. But I will tell you that even that statement is probably met with skepticism by some number of investors, media and policymakers. Indeed, based on recent events, I sometimes have my doubts, as well.

So, where does that lead us as we try to find a way forward in this environment of shattered trust? The regulators doubt the commitment of firms to operating at the highest ethical standards. The industry thinks the regulators have gone off the deep end and become competitors in a contest to see who can be toughest. And investors think neither the industry nor the regulators deserve their trust.

Speaking as a regulator, I think you will see us staying in the deep end for quite awhile. That means, above all else, aggressive enforcement of the rules and pushing enforcement of our bedrock ethical rule, **that firms must observe high standards of commercial honor and just and equitable principles of trade**. This means, among other things, that even where there isn't a specific rule tailored to address a specific situation, a firm and its officers should be committed to do the right thing.

It also suggests to me more creative sanctions in our enforcement cases, including taking a firm out of an entire line of business for a period of time when there have been repeated or particularly egregious violations. It is foreseeable that a full-service firm with multiple violations over a period of time in the mutual fund sales practice arena could be prohibited from opening any new mutual fund accounts for a period of time. The impact of such a sanction would be far greater than a fine of many millions of dollars and we have recently amended the NASD Sanction Guidelines to make clearer the capacity to have such sanctions considered.

Similarly, we will consider in the appropriate case, asking Board Compensation Committees of publicly owned broker-dealers to address how major regulatory failures were factored into their compensation decisions.



And, you will continue to see enforcement actions go up the chain of command and hold increasingly senior members of management responsible for the firm's transgressions as we did in September when we charged the national head of retail sales at a major firm for failure to supervise when regional and branch offices of the firm were holding illegal sales contests. Our decision in that case also talked extensively of the failure of the firm's Compliance Department to have any procedures to ensure compliance with the long-standing NASD rule prohibiting this type of sales contest.

This sort of lack of compliance and supervisory procedures has led me to ask our staff to step up the analysis of regulatory data which points to firms that are exhibiting red flags that enhanced compliance or supervision could address BEFORE there is a need for disciplinary action. We will be discussing our findings at face-to-face regulatory conferences with compliance officers and CEOs of firms, where we will also explore what remedial action is expected.

In a similar vein, this week, letters will be going out to firms that employ brokers with multiple customer complaints or other disclosures, reminding each firm of its responsibility to pursue heightened supervision with respect to the activities of these reps.

Recent events will probably control the tempo and tenor of future rulemaking for some time, as well. Most firms, and I would venture to say this is true in most industries, would prefer principle-based regulation in which the detail of policies and procedures is left to the firm to determine. And in principle, I agree this is a good goal for regulation wherever possible. But this approach becomes increasingly less possible when even a few firms demonstrate behavior that not only ignores the animating purpose of our rules but also flouts their express borders.

I think you can also expect to see the regulators demand more self-reporting from firms about their compliance weaknesses. And, as you know we are moving forward with certification from broker-dealers about the state of their compliance processes, not unlike the Sarbanes-Oxley certifications that require sign-off on financial statements and on the effectiveness of internal controls for financial reporting.

I can't predict for you what will happen in Congress, but I don't think anyone should yet count out mutual fund legislation this year, despite the many new requirements already proposed or enacted-and there will be more to come-concerning fund governance, and disclosure surrounding fees, soft dollars, and breakpoints, to name just a few.

On a more specific level, our focus on distribution and compensation issues related to mutual funds will continue through enforcement and rulemaking.

Our focus historically has been on the suitability of the mutual fund share classes that brokers recommend; the sales practices they employ; the disclosures they make to investors; and the compensation they receive from mutual funds. We also have played the lead role in policing whether brokers give customers the proper volume discounts-or breakpoints -off of the front-end "loads" that many funds levy, and we have lead the Task Force charged with developing the operational and regulatory changes necessary to prevent these problems in the future.

We will continue to monitor implementation of the Task Force recommendations and we have now expanded this line of inquiry into "discounts owed but not given," to UIT products and Net Asset Value Transfer programs.

Besides breakpoints, NASD has been highly active in mutual fund enforcement more broadly. Last year alone, we brought some 70 mutual fund cases-and more than 200 over the last three years covering

inappropriate share class sales, suitability and the use of directed brokerage commissions to pay for shelf space. There are nearly 200 ongoing, active investigations at NASD covering these fund-related issues, as well as market timing and late trading.

Let me just mention a couple of other areas where we will be highly focused this year.

I have long had concerns about how variable annuities are marketed to investors. We brought three important cases in the past month alone related to the sale of these products. We ordered Prudential to pay customers \$9.5 million and a \$2 million fine for variable annuity sales and switches that violated NY State Insurance Department regulations.

We filed a case earlier this year against Waddell & Reed and two of its senior executives charging them with recommending 6,700 variable annuity exchanges to its customers without determining the suitability of the transactions, generating \$37 million in commissions and costing their customers \$10 million in surrender fees.

The same week, we permanently barred from the industry, a Louisiana broker for unsuitable variable annuity sales.

While we have brought some 75 annuity-related disciplinary actions in the last three years, given the increasing complexity of these products and the impact of tax law changes, we will intensify our scrutiny. We are considering rulemaking in this area that could require pre-approval by a principal of the appropriateness of variable annuities in a manner akin to the process of approval for options trading, and we will consider whether firms must have their customers sign a specific risk disclosure document when considering an exchange of one variable annuity product for another.

Coming out of the Metropolitan case that we filed late last year, we are currently analyzing all securities offerings done over the past two years where a broker/dealer sold its own securities or those of an affiliate. Our examinations cover both registered offerings and private placements and include equity and debt. In case you missed the Metropolitan case, it involved fraud in the sale of debentures, investment certificates and preferred stock issued by two affiliated companies of an NASD member. The BD's sales force made unbalanced presentations to investors and downplayed important investment risk factors, including the risk of loss due to the companies' insufficient earnings, subordination of the securities to other obligations and the absence of an established market for the preferred stock.

We also have a growing concern about the intersection within broker-dealers of mortgage lending and securities investing. As investors have watched the tempting combination of a rising stock market, record low mortgage interest rates and tremendous growth in the equity they have in their homes, they have been tempted by sales pitches to unlock that equity, by refinancing their homes-perhaps through a non-registered affiliate of the broker/dealer-and investing the proceeds in the stock market.

So, I will go out on a limb here and say that 99% of the time, a recommendation that an investor mortgage his or her home in order to speculate in the securities market-IS UNSUITABLE-and subject to potential enforcement action.

We brought three enforcement cases last week against individual brokers for making unsuitable recommendations that included convincing clients to mortgage their houses.

Additional areas of interest that I can forecast for this year include debt and municipal security pricing and markups, retail sales of non-conventional products and an extensive effort, coordinated with the SEC and the NYSE to deal with abusive short-selling, to name just a few.

Before I finish, I'd like to go back to where I began: the role of the industry.

NASD will continue to be extraordinarily busy this year, as we have been for the last several years, but the harder task remains with the industry. I've outlined some of NASD's priorities and approach but in order to restore investor trust, what's truly critical is for brokerage firms to recommit to the principle of putting the investor first.

Brokers need to truly understand, accept and act on the fact that pursuing short-term profits, at the expense of treating your customers fairly will never be a successful strategy over the long run. Truthfully, I do not understand the failure to grasp and live this dynamic, particularly in the face of a thousand examples where it has been true.

The U.S. capital markets are the most efficient and resilient in the world because we operate in a market economy in which risk-taking that culminates in innovation, efficiency and consumer satisfaction is richly rewarded with profits. Regulators are not at war with profit seeking. But, profit seeking must not prevent any in this industry from honoring the responsibilities that arise from the trust placed in them by investors.

All commercial regulation reflects, at least in part, the understanding that unbridled capitalism can lead to excesses of behavior and harm, that we as a society find unacceptable. This is not a remarkable proposition. I believe I can presume to say that there is not a person in this room who does not believe that in the long term, you do better on the balance sheet by doing better for your customers.

I think that if the industry wants to preserve the privilege of self-regulation and to regain investor confidence and the confidence of regulators, then a cultural change is necessary at many firms.

There is a tendency in life to believe that the way things are is the way they will always be. This is why the end of bull markets are rarely seen. The way things were is not the way things can continue to be. I urge all of you to come to that realization. I believe it is as simple as this: if the industry wishes to be in control of its future it must control its conduct, it must act in the interests of its clients in deeds as well as words, and it must dispense with the notion that what is ethical can be informed by the formula of profit and loss.

This audience is composed of the best and the brightest, all of whom are committed to seeing fair markets thrive, investor interests served and healthy capitalism flourish. I urge you to redouble your efforts today and tomorrow in creating a strong, proactive culture of compliance within your firm that demonstrates that commitment to investors and regulators. There aren't any better uses of your time.



## RISK ALERT

DIVISION OF EXAMINATIONS

December 5, 2022

### **OBSERVATIONS FROM BROKER-DEALER AND INVESTMENT ADVISER COMPLIANCE EXAMINATIONS RELATED TO PREVENTION OF IDENTITY THEFT UNDER REGULATION S-ID<sup>1</sup>**

#### **I. Introduction**

This Risk Alert provides observations from recent examinations of SEC-registered investment advisers (“advisers”) and broker-dealers (together with advisers, “firms”) related to compliance with Regulation S-ID.<sup>2</sup> The Division of Examinations (“EXAMS”) is issuing this Risk Alert in order to assist firms with implementing effective policies and procedures under Regulation S-ID, which requires the development and implementation of an identity theft prevention program (“Program”) for firms that offer or maintain covered accounts.<sup>3</sup>

Regulation S-ID applies to SEC-regulated entities that qualify as financial institutions or creditors under the Fair Credit Reporting Act (“FCRA”)<sup>4</sup> and requires SEC-regulated financial institutions and creditors to determine whether they offer or maintain covered accounts. SEC-regulated entities that are likely to qualify as financial institutions or creditors and maintain

<sup>1</sup> The views expressed herein are those of the staff of the Division of Examinations, formerly known as the Office of Compliance Inspections and Examinations or OCIE (the “Division”). This Risk Alert is not a rule, regulation, or statement of the Securities and Exchange Commission (the “SEC” or the “Commission”). The Commission has neither approved nor disapproved the content of this Risk Alert. This Risk Alert has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person. This document was prepared by Division staff and is not legal advice.

<sup>2</sup> Regulation S-ID is set forth at 17 CFR 248.201 et. seq. Identity Theft Red Flags Rule, Joint Final Rules and Guidelines, Securities Exchange Act Release No. 34-69359, Investment Advisers Act Release 3582, Investment Company Act Release 30456 (Apr. 10, 2013), 78 FR 23637 (April 19, 2013) (“Identity Theft Red Flags Rule”), available at: <https://www.sec.gov/rules/final/2013/34-69359.pdf>.

<sup>3</sup> A “covered account” is (i) an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and (ii) any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. See 17 CFR 248.201(b)(3).

<sup>4</sup> Fair Credit Reporting Act, 15 U.S.C. 1681.

covered accounts include most registered broker-dealers (e.g., broker-dealers offering margin or custodial accounts) and registered investment companies (e.g., registered investment companies that allow individuals to wire transfers to other parties or that offer check writing privileges),<sup>5</sup> and some registered investment advisers (e.g., registered investment advisers who can direct transfers or payments from individual accounts to third parties based on the individual's instructions or who act as agents on behalf of individuals) if the accounts are primarily for personal, family, or household purposes.<sup>6</sup> If a firm determines that it has such accounts, it must establish a Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

## II. Most Frequently Observed Regulation S-ID Compliance Issues

Through its examinations, EXAMS staff identified practices that are inconsistent with the objectives of Regulation S-ID, which may leave retail customers vulnerable to identity theft and financial loss. Below are examples of the most common deficiencies identified by EXAMS staff in connection with the elements of Regulation S-ID.

### A. Identification of Covered Accounts

Under Regulation S-ID, firms must determine and then periodically reassess whether they offer or maintain covered accounts.<sup>7</sup> Accordingly, firms must conduct a risk assessment to determine whether they offer or maintain covered accounts, taking into consideration the methods they provide for opening and accessing accounts, as well as their previous experiences with identity theft. Below are examples of observations related to the periodic identification of covered accounts from recent examinations.

- ***Failure to identify covered accounts.*** EXAMS staff observed firms that failed to conduct an assessment of whether any of their accounts were “covered accounts” and as a result

<sup>5</sup> Regulation S-ID applies to any investment company that is registered or required to be registered under the Investment Company Act of 1940, that has elected to be regulated as a business development company under that Act, or that operates as an employees' securities company under that Act, if such investment company otherwise meets the definition of financial institution or creditor and offers or maintains covered accounts.

<sup>6</sup> See Identity Theft Red Flags Rule for additional examples of SEC-registered entities that may qualify as creditors or financial institution under FCRA. See also SEC Small Business Compliance Guide: Identity Theft Red Flags Rule, available at: <https://www.sec.gov/info/smallbus/secg/identity-theft-red-flag-secg.htm>.

<sup>7</sup> 17 CFR 248.201(c).

did not identify covered accounts at the firm and failed to implement a Program as required under Regulation S-ID.

- ***Failure to identify new and additional covered accounts.*** Some firms did initially identify, as covered accounts, one category of accounts that they offered, but they failed to conduct periodic assessments, either at all, or those periodic assessments did not identify all categories or new types of accounts that were “covered accounts.” For example, firms may have merged with other entities but then never conducted a reassessment to see whether any new accounts should be included in the Program. EXAMS staff observed examples of firms omitting online accounts, retirement accounts, and other special purpose accounts from firms’ determination and reassessment of covered accounts. EXAMS staff also observed instances where a firm did not maintain any documentation of their analysis of covered accounts. While not required by Regulation S-ID, such documentation can assist the firm in identifying the basis for their determination to auditors and regulators.
- ***Failure to conduct risk assessments.*** EXAMS staff also observed that while some firms periodically identified covered accounts, the process did not include a risk assessment taking into consideration the methods provided to open, maintain, and closed accounts; methods to access different types of covered accounts; or previous experiences with identity theft.<sup>8</sup> For example, in not periodically conducting a risk assessment of new methods to access accounts, some firms that historically maintained customer accounts at branch locations did not identify online accounts as covered under their Programs. This impacted firms’ abilities to develop controls relevant to their red flags.

## **B. Establishment of the Program**

Regulation S-ID requires firms to develop and implement a written Program that is appropriate to the size and complexity of the firm and the nature and scope of its activities.<sup>9</sup> Through recent examinations, EXAMS staff observed the following issues with respect to the establishment of written Programs.

<sup>8</sup> See Identity Theft Red Flags Rule at 27 (stating that “each financial institution or creditor must periodically determine whether it offers or maintains covered accounts”).

<sup>9</sup> 17 CFR 248.201(d)(1).

- ***Programs not tailored to the business.*** EXAMS staff observed firms that established a generic Program that was not tailored to or appropriate for their business model. In some cases, firms relied on a template with fill-in-the-blanks that had not been completed. Other firms adopted Programs that simply restated the requirements of the regulation without including processes for complying with the regulation.
- ***Program did not cover all required elements of Regulation S-ID.*** Firms represented to staff that other policies and procedures outside of a written Program constituted the firm's process for detecting, preventing, and mitigating identity theft, even though such procedures had not been incorporated directly or by reference into the Program and in many cases did not cover all of the required elements of Regulation S-ID.

### **C. Required Elements of the Program**

Programs under Regulation S-ID must include reasonable policies and procedures to identify, detect, and respond to red flags that are relevant to identity theft. Additionally, the Program must include reasonable policies and procedures to ensure that it is updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.<sup>10</sup> EXAMS staff observed the following instances in which Programs lacked required elements.

***Identification of Red Flags:*** Red flags are patterns, practices, or specific activities that indicate the possible existence of identity theft.<sup>11</sup> Programs must include reasonable policies and procedures to identify relevant red flags for covered accounts offered by the firm and incorporate those red flags into the Program. Supplement A to Regulation S-ID's Appendix A provides illustrative examples of red flags for a firm to consider. EXAMS staff observed firms that did not appear to have reasonable policies and procedures to identify relevant red flags. Specifically, EXAMS staff observed:

<sup>10</sup> 17 CFR 248.201(d)(2).

<sup>11</sup> 17 CFR 248.201(b)(10).

- Firms that failed to identify red flags specific to their covered accounts, and instead listed examples from Appendix A of Regulation S-ID regardless of the flags' relevance to the firm's covered accounts.
- Firms that only offered online accounts listed red flags related to the physical appearance of a customer; and some firms included red flags related to consumer reports even though those firms did not obtain consumer reports for customers.
- Firms that did not have a process or did not follow existing procedures to evaluate actual experiences with identity theft in order to determine if additional red flags should be added to their Programs. For example, EXAMS staff observed firms that experienced ongoing account takeovers over several years and did not consider any red flags related to account takeovers.
- Firms that did not include any identified red flags in their Program. For example, some firms created written Programs that had generic language for identifying, detecting and responding to, and updating red flags but the Programs did not include any actual red flags identified by the firms. As such, the written Programs were merely policy statements without any actionable procedures.

***Detect and Respond to Red Flags:*** Programs must have reasonable policies and procedures incorporated into the Program to detect and to respond appropriately to any red flags that are detected.<sup>12</sup> EXAMS staff observed firms that did not appear to have reasonable policies and procedures to detect and respond to relevant red flags. Specifically, EXAMS staff observed:

- Firms that relied on pre-existing policies and procedures (e.g., anti-money laundering procedures) to satisfy this requirement of its Program, when such procedures were not designed to detect and respond to identity theft red flags. For example, such procedures did not include processes to detect whether the fraud was related to identity theft, such as the use of forged or false credentials.
- Firms that identified procedures for detecting and responding to specific red flags, when the actual procedures did not exist or failed to contain any relevant process related to that

<sup>12</sup> 17 CFR 248.201(d)(2)(ii) and (iii).



red flag.

***Periodic Program Updates:*** Regulation S-ID requires that Programs include reasonable policies and procedures to ensure the Program is updated periodically to reflect changes in risks to customers and the firm from identity theft.<sup>13</sup> In recent examinations, EXAMS staff observed:

- Some firms did not update their identified red flags after making significant changes to the ways in which their customers open and access their accounts, such as providing account access not only through local branch offices, but also through online customer portals.
- Firms that had gone through business changes or reorganizations, such as mergers or acquisitions of other financial firms, but had failed either to incorporate these new business lines into their existing Program or to approve a new Program for these new business lines.

#### **D. Administration of the Program**

Firms must provide for the continued administration of the Program through (1) obtaining approval of the initial written Program from either its board of directors, an appropriate committee of the board of directors, or from a designated senior management employee, if the firm does not have a Board; (2) involving the board or senior management in the oversight and administration of the Program; (3) training staff as necessary; and (4) exercising appropriate oversight of service provider arrangements.<sup>14</sup> EXAMS staff observed firms that did not provide for the continued administration of their Programs as required by Regulation S-ID. For example:

- ***Did not appear to provide sufficient information to the board or designated senior management.*** EXAMS staff observed firms that did not appear to provide sufficient information to the board or designated senior management through periodic reports, either by failing to submit any reports or by submitting reports that did not appear to

<sup>13</sup> 17 CFR 248.201(d)(2)(iv).

<sup>14</sup> 17 CFR 248.201(e).

contain sufficient information for the board or senior management to evaluate the effectiveness of the Program.

- ***Inadequate Training.*** EXAMS staff observed firms that did not have robust processes to assess which employees should be trained, and some trainings appeared to be insufficient because the training was limited to a single sentence telling employees to be aware of identity theft.<sup>15</sup>
- ***Failure to evaluate controls of service providers.*** Some firms that relied on service providers to perform activities in connection with covered accounts did not evaluate the controls in place at the service provider to monitor for identity theft.

### III. Conclusion

In sharing these observations, EXAMS encourages registered broker-dealers and investment advisers to review their practices, policies, and procedures with respect to their Programs and to consider whether any improvements are necessary.

---

*This Risk Alert is intended to highlight for firms risks and issues that the Division's staff has identified. In addition, this Risk Alert describes risks that firms may consider to (1) assess their supervisory, compliance, and/or other risk management systems related to these risks, and (2) make any changes, as may be appropriate, to address or strengthen such systems. Other risks besides those described in this Risk Alert may be appropriate to consider, and some issues discussed in this Risk Alert may not be relevant to a particular firm's business. The adequacy of supervisory, compliance and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances.*

---

<sup>15</sup> 17 CFR 248.201(e)(3) (requiring firms to train staff to effectively implement the Program).

## Speech

---

# Anti-Money Laundering: An Often-Overlooked Cornerstone of Effective Compliance

**Kevin W. Goodman, National Associate Director, Broker-Dealer Examination Program, Office of Compliance Inspections and Examinations**

**Securities Industry and Financial Markets Association**

**June 18, 2015**

## Introduction

I would first like to thank our hosts, SIFMA, and everyone who worked so diligently to coordinate this conference. Before we begin, I would also like to state that my comments here today are mine and mine alone, and do not necessarily represent the views of the SEC, the Commissioners, or the Staff.<sup>[1]</sup>

I appreciate the opportunity to speak with you today about the critical importance of broker-dealers' anti-money laundering or "AML" programs. My speech is intended to further elaborate on a speech given by my colleague, Andrew Ceresney, on February 25, at SIFMA's recent AML conference, in which he highlighted the importance of strong AML programs.<sup>[2]</sup> I want to discuss Mr. Ceresney's remarks in the context of the role of OCIE's examination program, including how we will evaluate your firm's compliance with AML obligations.

As you all know, AML includes far more than just preventing traditional money laundering. Broker-dealers must report large cash transactions and retain records on wire transfers regardless of whether any potential criminal activity is suspected. Broker-dealers must also monitor for and report suspicious activity, including activity that has no business or apparent lawful purpose. This goes beyond activity that implicates drug cartels or terrorist rings – it also includes activity that might indicate fraud, insider trading, or manipulative trading schemes.

As you also know, OCIE expects you and your firms to implement robust compliance programs that are targeted to the specific risks at your firms, and AML is no exception.<sup>[3]</sup> In fact, implemented properly, I believe an AML compliance program can serve as a cornerstone of a firm's overall compliance program. AML, however, has important implications that proliferate far beyond your firms. Widespread AML lapses threaten our standing in the international community – not only for you as individual firms but for the United States as a whole.

In fulfilling their important AML obligations, broker-dealers play a vital front line role in assisting regulators and law enforcement in identifying and addressing suspicious activities to prevent our financial systems from being used for criminal purposes. Your obligation is a proactive one, not a ministerial one. OCIE strives to be transparent about our focus areas and concerns, so I want to highlight that we take AML very seriously and will take great exception to firms that view AML as a peripheral or unimportant component of their compliance program. Quite the opposite in fact, I believe that a minimal or weak AML program implicates the entire compliance program, while a strong AML program can serve as the cornerstone.

In the absence of regular risk assessments as to how your firm could be used by sophisticated individuals and entities seeking to evade the law, it is difficult to know how you could meet your critically important AML obligations. It isn't enough to say that your firm did not have intent to break the law, that you did not know what a customer was doing, that you relied on a vendor's system that other firms have found useful, or that the information was gathered and reviewed for other surveillance purposes.<sup>[4]</sup> Your firm must be able to demonstrate that it has an AML program that is tailored to the risks posed by your business and customers.<sup>[5]</sup> I challenge you here today to think beyond technical compliance and to consider your AML responsibilities as critical to your firm and to our financial system.

With that backdrop, today I plan to discuss the main components of an AML program, what factors you may want to consider in evaluating your program's adequacy, what examiners will be looking for, and where the SEC and other regulators have found deficiencies. In particular, I will highlight innovative methods that we are using to detect weaknesses in broker-dealers' AML programs. I want to encourage you to evaluate your current program against the points I raise today so that when OCIE examiners walk in your door, they will find a robust AML program that is worthy of the important gatekeeper role you play.

## Significance of AML <sup>[6]</sup>

While at first blush AML obligations may seem to be the mechanical process of monitoring and reporting cash flows and securities transactions, AML programs are actually much more. <sup>[7]</sup> When implemented well, they provide protections against misuse of the nation's financial system for criminal activity – activity that ranges from financial fraud (endangering people's financial security) to profiting from drug businesses to funding terrorist activities. For example, federal authorities have used filed suspicious activity reports ("SARs") to identify fraud schemes such as purported investments in non-existent high yield investments, Ponzi or pyramid schemes, and market manipulation.<sup>[8]</sup> In describing how the SEC's Enforcement Division will assess SARs, Mr. Ceresney noted that SARs reporting "contributes directly to our work at the SEC to protect investors and ensure that our markets operate fairly," and he identified the many times when SARs played a part in SEC regulatory actions as well as prompted examinations and investigations.

It is therefore understandable that when firms are not meeting their obligations, the consequences are severe. I point to two recent cases that, while not brought against broker-dealers, illustrate lessons that, I believe, can and should be learned by all firms. I would add that the SEC has also brought several actions against broker-dealers for violations in the AML arena, some of which I will discuss in a few minutes.

In 2012, HSBC Bank USA settled claims with regulators, including the Financial Crimes Enforcement Network – or FinCEN, the bureau of Treasury charged with implementing the Bank Secrecy Act or BSA, with penalties exceeding \$1.9 billion for failure to have an adequate AML program.<sup>[9]</sup> Regulators raised concerns of an understaffed AML compliance function, a failure to monitor numerous transactions from high risk jurisdictions, and even the classification of one such jurisdiction as the lowest AML risk category. FinCEN's assessment stated over and over again that HSBC's fundamental flaw was a failure to conduct risk-based evaluations in designing its program – ignoring the need to evaluate the risks of products and services offered, its customer base, and countries from and to which moneys flowed. So, I suggest to you that conducting an overall analysis of the risk posed by your business is a critical step towards implementing an effective AML program where you employ adequate resources and put them where they are needed the most. And, please be sure that you are providing resources commensurate with the risks identified.

In a second more recent case (January 2014), J.P. Morgan paid a \$1.7 billion fine for its failures to report suspicious activity relating to the Bernard Madoff Ponzi scheme.<sup>[10]</sup> Between 1986 and 2008, the scheme was conducted almost exclusively through accounts at J.P. Morgan Chase Bank. Over a multi-year period, multiple red flags were identified. J.P. Morgan was concerned enough that it reduced its financial exposure to Madoff funds in response to those red flags. However, even after J.P. Morgan's UK affiliate reported its concerns to the U.K. authorities, no such report was made in the U.S. In part, this failure appears to have resulted from communication

lapses between business and compliance, and between different compliance groups. So, what is the lesson learned here? Note that having a sophisticated surveillance system alone did not satisfy the firm's obligations. You need to know that all relevant information is flowing through to the employees with responsibility to file SARs.

Now, I'll focus on where broker-dealers have faced regulatory action for failing to meet their AML obligations. The Commission has brought multiple cases against firms such as Hold Brothers, Biremis, Park Financial Group, and Gilford, among others, in which customers or employees of a broker-dealer engaged in manipulative trading schemes – layering,<sup>[11]</sup> pump and dump schemes,<sup>[12]</sup> and/or sales of unregistered shares.<sup>[13]</sup> Each of these cases is fact specific but all have a common theme: broker-dealers had multiple red flags brought to their attention – whether it be a customer's explanation of trading that didn't align with the facts, a large quantity of low-priced shares deposited at the broker-dealer, or the absence of information about the customer – and the firm's personnel essentially ignored red flags, with severe consequences, including bars from the securities industry and significant fines against the firm and firm personnel.

## AML Requirements

I would now like to walk through three major AML requirements – the AML compliance program, the customer identification program, and monitoring and reporting suspicious activity. I will provide some color on steps examiners will take in their review. I will also highlight certain regulatory actions that provide examples of where firms have gone wrong. I would suggest as a take-away that firms assume unacceptable risk when they fail to consider the characteristics of the businesses in which they are engaged, and I emphasize the need to evaluate your business activities, the unique risks they present, and what controls would be reasonable to address these risks.

### AML Compliance Program

FINRA Rule 3310 requires members to establish a risk-based AML compliance program, which includes at a minimum, reasonably designed policies and procedures, the designation of an AML compliance officer, ongoing AML employee training, and independent testing of the AML program.<sup>[14]</sup> I also echo Mr. Ceresney's statement that "it is critical to ensure that AML compliance is integrated fully into the other compliance operations of the firm to ensure that suspicious activity detected by other compliance functions makes its way to the AML compliance function and vice versa."

Examiners will begin by evaluating whether your program is reasonably designed. In our examiners' experience, the "reasonably designed" standard is not met where firms rely on boiler-plate language or templates or "off-the-shelf" programs that are not tailored to their customers, products, services, geographic locations, or methods of customer interface. Firms should also be aware of when its automated programs are not operating correctly and should confirm that any technical fixes to the program are appropriate.<sup>[15]</sup> Examiners assess the capacity of designated compliance officers, including their background and experience and whether they have the resources to perform their jobs adequately. Examiners consider whether the training provided to employees takes into account the function being performed by the employee, the specific business activities of the firm, and the specific AML program of the firm. I would caution against the use of generic training that does not explain to employees the specific roles and responsibilities that they have.<sup>[16]</sup> OCIE expects that the scope of independent testing reasonably covers the lines of business in which your firm engages.<sup>[17]</sup> Finally, we expect to see documentation of the independent testing performed on the effectiveness of your AML program. A simple sign-off that the testing occurred is almost never deemed compliant;<sup>[18]</sup> it should specify the testing conducted and the results.

You might take a look at the Brown Brothers Harriman case settled with FINRA in February 2014, to see the application of FINRA Rule 3310 and, in particular, the need for an AML program tailored to the specific risks that a firm faces.<sup>[19]</sup> The case involved omnibus accounts being used to conduct penny stock transactions for undisclosed underlying customers of foreign banks, and the broker-dealer's inability to obtain critical information such as the identity of the stock's beneficial owner, how the stock was obtained, and the owner's relationship with

the issuer. I believe this case illustrates the need to identify and address high risk business activities – such as penny stock trading. You might also consider the concerns raised by omnibus accounts or other instances (such as DBA or “doing business as” accounts) in which an entity trades through different names, and how it impacts your ability to monitor trading in a meaningful fashion. Finally, you might also want to consider that FINRA discussed that the firm’s failure to review its penny stock activities flowed through multiple aspects of its AML program – with gaps in its monitoring, independent testing, and employee training. So, the cases show that you not only need to identify the high risk areas, you need to tailor each AML control component accordingly.

I also want to point you to a case brought by FinCEN against a broker-dealer, Oppenheimer & Company, in 2005, which settled for \$2.8 million.<sup>[20]</sup> FinCEN charges were based on Oppenheimer’s failure to have an adequate AML program, including an absence of procedures for reviewing wire transfer and journal transactions between unrelated and related customer accounts from foreign branch offices; reliance on manual review of transactions by one employee; reports that did not aggregate incoming and outgoing wire transfers by customer, account, branch office, or destination; and a lack of independent testing of the effectiveness of the program. Moving ahead about 10 years, Oppenheimer once again is the subject of significant AML enforcement actions, one brought by FINRA and settled for \$1.425 million, and one brought by the SEC and settled for \$20 million, both resulting from failing to detect and report suspicious transactions in connection with unregistered sales of penny stock.<sup>[21]</sup> So please be mindful of regularly assessing and reassessing the risks your firm faces and its compliance with the regulatory framework.

## CIP Program

The second fundamental AML obligation is that broker-dealers must implement a customer identification program (or “CIP”) to obtain all of the required information – the name, address, date of birth for an individual, and identification number – for each customer and have a method to verify that information.<sup>[22]</sup> Examiners will review a firm’s verification policies and procedures to ensure they are reasonable given the firm’s assessment of the risk factors associated with its customer base. Further, examiners will be looking to ensure firms correctly understand and are meeting their CIP obligations for anyone who qualifies as a customer – that is, generally, a person who establishes a formal relationship with your firm to effect transactions in securities.<sup>[23]</sup> You and your firms should give careful consideration as to whether each of the businesses you’re engaging in triggers the CIP requirements. For example, to give some color as to when a person might be a customer for BSA purposes, FINRA has taken action against firms whose CIP programs did not capture persons who purchased securities from the broker-dealers in private placements.<sup>[24]</sup>

I also refer you to the SEC’s settled action against Pinnacle Capital Markets.<sup>[25]</sup> Pinnacle primarily engaged in providing direct market access to its customers, 99% of which resided outside the United States. Pinnacle’s direct customers sometimes offered subaccounts to other entities to trade through Pinnacle. Pinnacle failed to conduct CIP reviews of the subaccount holders. An important point highlighted by this case is that omnibus sub-account holders were considered customers under the CIP rule because Pinnacle treated the sub-account holders in the same manner as it did its regular account holders, allowing them to use direct market access software to enter securities trades with Pinnacle directly and instantly through their own computer. These sub-account holders had direct control over how the trades were made in their accounts and did not require the omnibus account holder to initiate or intermediate the transactions. Again, I would suggest that the takeaway here is that you should carefully evaluate who is covered under your CIP – have you taken into account not just direct customers but other persons who may effect securities transactions directly to or through your firm?

## Detecting and Reporting Suspicious Activity

Detecting and reporting suspicious activity is a third fundamental aspect of AML compliance because, as set forth by Mr. Ceresney, the information you and your firms provide to regulators and law enforcement in SARs plays a vital role in helping regulators identify securities violations and bad actors in the markets. The SAR rule requires broker-dealers to report suspicious activity that involves or aggregates funds or other assets of at least \$5,000 and

for which the broker-dealer knows, suspects, or has reason to suspect: 1) involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade **any Federal law or regulation**, 2) is designed to evade any requirement of the Bank Secrecy Act, 3) has no apparent business or lawful purpose or is not the sort of activity in which the particular customer would normally be expected to engage, or 4) involves the use of the firm to facilitate criminal activity. [26] Once again I note that this goes far beyond traditional money laundering or terrorist financing.

Under this rule, in identifying activity with “no apparent business or lawful purpose,” you should question trading activity that does not have a discernible investment or profit objective, companies with complex ownership structures that transfer money between accounts with unclear objectives, or the use of front companies to hide illicit sources of funds. Important red flags include the use of securities accounts for predominantly non-securities related types of transactions (e.g., wire transfers) and customers who seem to not care about high fees or losses in their accounts and appear more focused on the movement of funds. [27] Broker-dealers with significant online access channels may want to take into account the source of login transmissions, particularly use of anonymous Internet nodes.

Examiners will evaluate whether firms are using monitoring processes and tools commensurate with the volume and types of activity occurring in accounts. Examiners will test the thresholds, parameters, and the data that is fed into automated systems for SAR monitoring, as well as look at the process by which AML alerts coming from these automated systems are reviewed and escalated.

For further color on when SARs reporting may be required, you should look to the SEC’s actions in Gilford Securities, [28] Hold Brothers On-Line Investment Services, [29] and Bloomfield. [30] In each case, the firm did not file SARs even though firm personnel knew or should have known about activity that indicated potential market manipulation such as a pump and dump scheme, layering, or artificially raising the market price of a thinly traded security. Both the HSBC and JP Morgan actions also included charges of failures to file SARs. I cannot emphasize enough the importance of filing SARs, and it is no coincidence that both Mr. Ceresney’s and my remarks highlight this aspect of AML compliance. With that, I will turn to OCIE’s efforts to address failures to file SARs.

## AML Examination Initiatives

Mr. Ceresney’s remarks provided an excellent analysis of how the SEC reviews SARs filings and the concerns raised by filings that do not provide sufficient detail. He also identified statistics that raise red flags for me as well. On average, each firm in the U.S. files about five SARs a year. A large number of firms file zero or one SAR per year. I agree with Mr. Ceresney’s statement that it is “hard to believe that the industry as a whole is fulfilling its obligation,” and OCIE is looking into whether firms are filing SARs appropriately. Mr. Ceresney in his speech outlined the Enforcement initiatives to address this concern, I will focus now on where the examination program is directing its resources.

Because examiners are forced to be risk-based in their reviews, one particular area of focus will be the AML programs of clearing firms. OCIE believes that those institutions often have the “birds-eye view” of the market and are in the best position to identify patterns of activity engaged in by persons or entities that use more than one introducing broker. Examiners would expect clearing firms to use that high-level view of trading to monitor for suspicious patterns and report the activity on SARs. [31] During examinations of clearing firms, examiners, too, are able to review activity transacted through a large number of broker-dealers. Examiners can then select introducing broker-dealer(s) for targeted, risk-based examinations based on the analysis, which may take into account concerns about whether the introducing firms appropriately reported suspicious activity. Remember, under the legal requirements, both the introducing firm and the clearing firm have responsibilities to detect and report suspicious activity that occurs by, at, or through their firm. Among other concerns, clearing firms should consider whether SARs should be filed if they identify trading patterns that may indicate potentially fraudulent activity such as churning of customer accounts or manipulation of the prices of microcap stock.



In choosing firms to examine for AML compliance, staff uses technology to identify firms that do not file or rarely file SARs, and we assess whether those firms have robust AML programs and monitoring processes in place. We assess the quality of SARs filed to ensure that firms are reporting in a meaningful enough way for the information to be helpful to the regulatory and law enforcement communities. For example, a SAR that identifies a possible Ponzi or insider trading scheme is most helpful when it includes the underlying information or transaction detail on which the firm is raising the concern. As another example, a SAR that reports thinly traded securities being deposited into an account and immediately sold for a large profit is most helpful if the SAR also provides how much the security was purchased for, when it was purchased, and who the shares are being sold to in the reported transaction. Note that FinCEN has provided guidance that stresses the need to file a complete and sufficient SAR. [32]

Examiners are also using enhanced data analytics and pattern recognition to evaluate whether broker-dealers are reasonably monitoring and reporting suspicious activity. The algorithms aren't being used to set a standard but rather to check the reasonableness of the parameters set by firms. We are increasingly incorporating into our reviews enhanced technology and tools to review vast amounts of data so that we can identify suspicious activity from the source trade data rather than relying on the broker-dealer's surveillance reports. We compare the activity we identify to activity identified by the firm, to test for weaknesses in a firm's monitoring and reporting of suspicious activity. Examiners are assessing the tools used by firms, including the firm's ability to detect patterns of customer activity and customers' aggregate activity, taking into account such factors as activity across related business and individual accounts and aggregation based on known beneficial owners. We are also planning to build learning algorithms, or artificial intelligence-like programs, that can help to identify the behavior trends of potentially illicit actors.

## Areas of Focus

I would now like to highlight a few business activities that OCIE has identified as potential sources of AML concerns. While some of these products and services or account relationships may not be inherently suspicious or high risk, they do present vulnerabilities that firms need to address from an AML perspective.

### Thinly Traded or Low Market Value Securities

Broker-dealers that provide services related to thinly traded or low market value securities need to consider the risks involved in such products. For example, the market price for these securities is often subject to significant fluctuations, and such companies have been in the past the target of spam campaigns to "pump" up the price, with quick sales to take advantage of the inflated market value. [33] Firms should evaluate whether they have controls to identify suspicious activity such as deposits of large quantities of shares followed by immediate sales, frequent transactions between accounts, or ties between the account holder and parties with a relationship to the company. [34] Such activities may require that you file a SAR. Recently, OCIE has issued a National Exam Program Risk Alert that provides insight into issues and risks that broker-dealers might face when their customers actively trade low priced securities. [35] The alert highlights trading patterns that might trigger the need to file a SAR and omnibus account types that appeared to be frequently associated with unregistered sales of low priced securities. I urge you to review this risk alert and consider whether your AML program has appropriately taken into account the concerns raised in designing appropriate controls.

### Direct Market Access

OCIE's 2015 Examination Priorities Memo [36] identified as a focus area the AML programs of proprietary trading firms that allow customers to directly access the markets from higher risk jurisdictions. In November 2010, the Commission adopted Exchange Act Rule 15c3-5, which requires broker-dealers that provide customers with direct market access to adopt a system of risk management controls, including restricting access to persons and accounts pre-approved and authorized by the broker-dealer. Broker-dealers offering these services should carefully evaluate how it may impact their CIP and SARs monitoring obligations. [37] Your obligation to report



suspicious activity is based on transactions that are conducted “by, at, or through” the firm, which includes direct market access activity. In addition, as discussed in the Pinnacle action I cited earlier, entities granted trading privileges at your firm may be customers under the CIP rule. So, we would expect to see reasonably designed controls to address these activities.

You may want to read closely the SEC’s action and FINRA’s allegations in its complaint against Wedbush Securities, which provide good sources of potential AML issues to consider for broker-dealers offering direct market access. [38] In particular, broker-dealers should consider whether their AML policies and procedures are tailored to their market access business, including monitoring for layering, spoofing, and other forms of manipulation, and that SARs are appropriately filed to respond to such activity.

## Master/Sub Account Relationships

In 2011, OCIE issued a risk alert that identified the master/sub account trading model as a vehicle that could be used to further violations of securities laws as well as other laws and regulations, including AML.[39] The 2014 risk alert that I referenced above on low priced securities identified master/sub accounts as structures that may be used in unregistered sales of low priced securities. OCIE remains concerned about consistent application of suspicious activity monitoring and reporting relating to master/sub account relationships.

In a master/sub account, a company opens up a brokerage account or master account through which numerous individuals or other entities are allowed to trade as sub account holders. In some reviews conducted by staff, as identified in the risk alert, the broker-dealer did not know the identity of the sub account holders. The respective introducing and/or clearing firm holding the master account, although generally aware of the master/sub account structure, may be monitoring solely on the aggregate master account activity and either ignoring red flags or failing to monitor the patterns of sub account activity. Firms that offer master/sub arrangements are reminded that the SAR rule, unlike the CIP rule, is not a customer-driven rule, but rather a transaction-driven rule. Failure to adequately monitor for activity occurring through the firm because such monitoring is done solely on an account or direct customer basis may put firms at risk for AML deficiencies.[40] What this means is that although you may find, based on your analysis of your business, that a person may not be a ‘customer’ of your firm and hence does not trigger the CIP requirement, you are nevertheless obligated to monitor any transaction occurring by, at or through your firm on behalf of that person.

## Banking-Oriented Products and Services

Examiners will evaluate the use of brokerage accounts that offer “comprehensive asset management” or “cash management” features. These accounts may present new avenues for potential money laundering. They allow customers to engage in not only securities transactions but also offer products and services traditionally associated with bank accounts, such as check writing ability, journaling among accounts, debit card/ATM access, credit cards, credit-line cash advances, ACH electronic funds transfers, and wire transfers. Firms that offer these services need to account for all of these transactional capabilities when reasonably designing an AML program. [41]

Examiners will assess all transaction methods for movement of cash and securities and testing the SAR monitoring thresholds accordingly to check for consistency with the firm’s obligations. Staff will look for monitoring that captures patterns of activity; aggregate activity; structuring of currency transactions to attempt to evade reporting and recordkeeping obligations; securities accounts that only have money movements and no securities investments; high-frequency check-writing, journaling, and wiring funds; and other activity that is not commensurate with a customer’s stated business or investment objectives.

Examiners have identified certain customers of firms that are using comprehensive asset management accounts as traditional retail banking or demand deposit relationships. Broker-dealers’ transaction monitoring program should, I believe, take into account how such accounts are being used. For example, if the account is being used primarily for banking rather than securities services, the firm should understand why the customer is holding funds

in a securities account rather than a traditional banking account. For business accounts and personal accounts that are being used for commercial purposes, our examiners will determine how much your firms know about the purpose for which the account is being used by the customer (e.g., what products and services your customer is offering). If you do not know enough about your customer's businesses, you may not be in a position to determine if the activity is consistent with that business type, size, and location.

## Conclusion

Today, I have highlighted some of the many challenges you all face in designing and implementing effective AML programs and the critical importance of meeting these challenges. Let's recap some of the major considerations in the process:

- You must analyze the risks associated with your business activities – understand which products and services have higher risks and/or require unique controls and consider geographic locations and methods of customer interface – and take this analysis into account in designing your AML program;
- You must have an adequately staffed AML compliance function with appropriate information flows and an effective escalation process;
- You must document your program in written procedures and be able to demonstrate the monitoring and the testing that occurs;
- You must understand the scope of activities that may need to be reviewed and in particular consider that SAR reporting is based on all transactional activities that run through your firm; and your CIP may need to include indirect customers if they have unintermediated ability to direct trading in an account held at your firm;
- For most firms, you must have a well-tailored electronic system to spot red flags among your thousands (or even millions) of daily transactions, and your staff must properly follow-up to determine whether the red flags must be reported on a SAR; and
- Finally, and perhaps most importantly – always consider the need to file SARs. Don't fail to file because you believe that the activity has been reported by someone else or that you don't have definitive proof that illegal activity has occurred or you have reported the activity through other channels – you are still required to file a SAR in these instances. Essentially, if you see activity that raises concerns or which you can't explain, we would encourage you to file a report. Also note that the SEC has established a SAR alert message line to be used when a filed SAR may require immediate attention (202-551-SARs).

Let me close by reiterating that AML compliance is an especially critical component of a firm's overall compliance program, the cornerstone over which all else is built. To design and implement effective AML programs, I encourage all of you to share information and approaches with one another to promote the development of the critical infrastructure that is needed and required. Investors and citizens deserve nothing less.

Please feel free to reach out to Commission staff within the Division of Trading and Markets and OCIE with any issues you want to discuss. We stand ready to do what we can to assist you in meeting your AML obligations.

Thank you again for your time and attention.

---

[1] The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed herein are those of the author and do not necessarily reflect the views of the Commission or of the author's colleagues upon the staff of the Commission.

[2] Available at: <http://www.sec.gov/news/speech/022515-spchc.html>.

- [3] See, e.g., FINRA Rules 3130 and 3310; 31 C.F.R. 1023.210 (The AML program rule of the Financial Crimes Enforcement Network or FinCEN applicable to broker-dealers) and 31 C.F.R. 1010.810 (FinCEN's rule delegating authority to the SEC to examine broker-dealers for compliance with applicable FinCEN regulations).
- [4] See, e.g., In the matter of Park Financial Group, Inc., Exchange Act Release No. 56902 (Dec. 5, 2007), *available at* <http://www.sec.gov/litigation/admin/2007/34-56902.pdf> (settled matter); In the matter of Hold Brothers On-Line Investment Services, LLC, Exchange Act Release No. 67924 (Sept. 25, 2012), *available at* <http://www.sec.gov/litigation/admin/2012/34-67924.pdf> (settled matter); In the matter of Biremis Corporation, Exchange Act Release No. 68456 (Dec. 18, 2012), *available at* <https://www.sec.gov/litigation/admin/2012/34-68456.pdf> (settled matter); FINRA Letter of Acceptance, Waiver and Consent No. 2010025241301 Re: Banorte-Ixe Securities International, Ltd. (Jan. 28, 2014), *available at*: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=35121>; FINRA Letter of Acceptance, Waiver and Consent No. 2012034123501 Re: Wells Fargo Advisors, LLC, and Wells Fargo Advisors Financial Network, LLC (Dec. 18, 2014), *available at*: <http://disciplinaryactions.finra.org/Search/ViewDocument/38254>. National Money Laundering Risk Assessment 2015 ("NML Risk Assessment") Department of Treasury (June 12, 2015), at pages 82-84, *available at*: <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>.
- [5] See, e.g., FINRA Letter of Acceptance, Waiver and Consent No. 2010025241301 Re: Banorte-Ixe Securities International, Ltd. (Jan. 28, 2014), *available at*: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=35121>.
- [6] For links to all of the legal and regulatory sources referenced here, see Anti-Money Laundering Source Tool for Broker-Dealers, *available at*: <http://www.sec.gov/about/offices/ocie/amlsourcetool.htm#1>.
- [7] In 1970, the Currency and Foreign Transactions Reporting Act of 1970, commonly known as the "Bank Secrecy Act" was enacted to require certain reports and records that have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings. The full complement of AML requirements came into effect with the USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), which amended the Bank Secrecy Act. The Patriot Act was passed shortly after 9/11 to prevent the use of the U.S. financial system to aid terrorist activities. In the securities sector, the Treasury Department, along with the SEC and FINRA, has implemented these requirements by adopting rules addressing broker-dealers' and mutual funds' obligations to combat money laundering and terrorist financing, which require firms to implement a risk-based AML compliance program and a customer identification program, to monitor and report suspicious activity, and to conduct due diligence on foreign correspondent accounts and private banking accounts. 31 CFR Parts 1023 (broker-dealers) and 1024 (mutual funds). Broker-dealers' obligations to file reports and maintain records pursuant to these requirements are also reflected in Exchange Act Rule 17a-8.
- [8] Examples of cases identified through the use of SARS *available at*: [http://www.fincen.gov/news\\_room/rp/sar\\_case\\_example\\_list.html?catid=00002](http://www.fincen.gov/news_room/rp/sar_case_example_list.html?catid=00002).
- [9] FinCEN's assessment is set forth in: In the matter of HSBC Bank USA N.A., Case Number 2012-02 (Dec. 10, 2012), *available at*: [http://www.fincen.gov/news\\_room/ea/files/HSBC\\_ASSESSMENT.pdf](http://www.fincen.gov/news_room/ea/files/HSBC_ASSESSMENT.pdf).
- [10] FinCEN's assessment is set forth in: In the matter of JPMorgan Chase Bank, N.A., Case Number 2014-1 (Jan. 7, 2014), *available at*: [http://www.fincen.gov/news\\_room/ea/files/JPMorgan\\_ASSESSMENT\\_01072014.pdf](http://www.fincen.gov/news_room/ea/files/JPMorgan_ASSESSMENT_01072014.pdf).
- [11] In the matter of Hold Brothers On-Line Investment Services, LLC, Exchange Act Release No. 67924 (Sept. 25, 2012), *available at* <http://www.sec.gov/litigation/admin/2012/34-67924.pdf> (settled matter); In the matter of Biremis Corporation, Exchange Act Release No. 68456 (Dec. 18, 2012), *available at* <https://www.sec.gov/litigation/admin/2012/34-68456.pdf> (settled matter).

[12] In the matter of Park Financial Group, Inc., Exchange Act Release No. 56902 (Dec. 5, 2007), *available at* <http://www.sec.gov/litigation/admin/2007/34-56902.pdf> (settled matter).

[13] In the matter of Gilford Securities, Incorporated, Exchange Act Release No. 65450 (Sept. 30, 2011), *available at* <https://www.sec.gov/litigation/admin/2011/33-9264.pdf> (settled matter); In the matter of Ronald S. Bloomfield, Robert Gorgia, and John Earl Martin, Sr, Exchange Act Release No. 71632 (Feb. 27, 2014), *available at* <http://www.sec.gov/litigation/opinions/2014/33-9553.pdf>.

[14] NASD Rule 3011 was adopted in 2002. In 2010, FINRA Rule 3310 replaced NASD Rule 3011.

[15] See, e.g., FINRA Letter of Acceptance, Waiver and Consent No. 2012034123501 Re: Wells Fargo Advisors, LLC, and Wells Fargo Advisors Financial Network, LLC (Dec. 18, 2014), *available at*: <http://disciplinaryactions.finra.org/Search/ViewDocument/38254>, in which FINRA brought an action under FINRA Rule 3310, later settled for \$1.5 million, based on a design flaw in the transaction processing system that resulted in certain customer accounts not being analyzed under the customer identification program.

[16] See, e.g., Letter of Acceptance, Waiver and Consent No. 2013035821401 re Brown Brothers Harriman & Co. (Feb. 4, 2014), *available at*: <http://disciplinaryactions.finra.org/Search/ViewDocument/35225>; NML Risk Assessment at pages 82-84, *available at*: <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>; Letter of Acceptance, Waiver and Consent No. 2010021211901 re Firstrate Securities, Inc. (May 7, 2013), *available at*: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=33515>; In the matter of Biremis Corporation, Exchange Act Release No. 68456 (Dec. 18, 2012), *available at* <https://www.sec.gov/litigation/admin/2012/34-68456.pdf> (settled matter); Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007 (August 11, 2014), *available at* [http://www.fincen.gov/statutes\\_regs/guidance/pdf/FIN-2014-A007.pdf](http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2014-A007.pdf).

[17] See, e.g., Letter of Acceptance, Waiver and Consent No. 2013035821401 re Brown Brothers Harriman & Co. (Feb. 4, 2014), *available at*: <http://disciplinaryactions.finra.org/Search/ViewDocument/35225>.

[18] See, e.g., Letter of Acceptance, Waiver and Consent No. 2010021162202 re Biremis Corp. (June 20, 2012), *available at*: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=32132>.

[19] Letter of Acceptance, Waiver and Consent No. 2013035821401 (Feb. 4, 2014), *available at*: <http://www.finra.org/web/groups/industry/@ip/@enf/@ad/documents/industry/p443448.pdf>.

[20] In the matter of Oppenheimer & Company, Case Number 2005-4 (Dec. 29, 2005), *available at* [http://www.fincen.gov/news\\_room/ea/files/oppenheimerassessment.pdf](http://www.fincen.gov/news_room/ea/files/oppenheimerassessment.pdf).

[21] Dept. of Enforcement v. Oppenheimer & Co., Inc., Order Accepting Offer of Settlement (Aug. 5, 2013), *available at*: <http://disciplinaryactions.finra.org/Search/ViewDocument/33961>; In the matter of Oppenheimer & Co. Inc., Exchange Act Release No. 74141 (Jan. 27, 2015), *available at*: <http://www.sec.gov/litigation/admin/2015/33-9711.pdf>.

[22] 31 C.F.R. 1023.220.

[23] 31 C.F.R. 1023.100(a)(d)(1). Staffs of the Treasury and the Commission issued a question and answer that identified the following specific fact pattern in which a beneficial owner of an omnibus account or subaccount is not considered a customer: if (1) the omnibus account or relationship is established by or on behalf of a financial intermediary for the purpose of executing transactions that will clear or settle at another financial institution, or the omnibus accountholder provides limited information to the broker-dealer solely for the purpose of delivering assets to the custody account of the beneficial owner at another financial institution; (2) the limited information given to the broker-dealer about the beneficial owner is used primarily to assist the financial intermediary with recordkeeping or to establish sub-accounts that hold positions for a limited duration to facilitate the transfer of assets to another financial institution; (3) all transactions in the omnibus account or sub-accounts at the broker-

dealer are initiated by the financial intermediary; and (4) the beneficial owner has no direct control over the omnibus account or sub-accounts at the broker-dealer. Guidance *available at*:

<https://www.sec.gov/divisions/marketreg/qa-bdidprogram.htm>.

[24] FINRA Letter of Acceptance, Waiver and Consent No. 2012030436201 Re LWB Investment Services, LLC (July 10, 2014), *available at*: <http://disciplinaryactions.finra.org/viewDocument.aspx?DocNb=36727>; FINRA Letter of Acceptance, Waiver and Consent No. 2010021128601 Re The Carson Medlin Company (Nov. 30, 2011), *available at*: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=27408>.

[25] In the matter of Pinnacle Capital Markets LLC, Exchange Act Release No. 62811 (Sept. 1, 2010), *available at* <http://www.sec.gov/litigation/admin/2010/34-62811.pdf>.

[26] 31 C.F.R. 1023.320.

[27] NASD Notice to Members 02-21 (April 2002) <http://www.sec.gov/about/offices/ocie/aml2007/nasd-ntm-02-21.pdf>.

[28] In the matter of Gilford Securities, Incorporated, Exchange Act Release No. 65450 (Sept. 30, 2011), *available at*: <https://www.sec.gov/litigation/admin/2011/33-9264.pdf> (settled matter).

[29] In the matter of Hold Brother On-Line Investment Services, Exchange Act Release No. 67924 (Sept. 25, 2012), *available at*: <http://www.sec.gov/litigation/admin/2012/34-67924.pdf> (settled matter).

[30] In the matter of Ronald S. Bloomfield, Robert Gorgia, and John Earl Martin, Sr, Exchange Act Release No. 71632 (Feb. 27, 2014), *available at*: <http://www.sec.gov/litigation/opinions/2014/33-9553.pdf>.

[31] Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations FIN-2008-G002 (March 4, 2008) (“a clearing firm’s anti-money laundering program should contain risk-based policies, procedures, and controls for assessing the money laundering risk posed by its fully disclosed clearing arrangements, for monitoring and mitigating that risk, and for detecting and reporting suspicious activity”), *available at*: <http://www.sec.gov/about/offices/ocie/aml/fin-2008-g002.pdf>. See, also, FINRA Letter of Acceptance, Waiver and Consent No. 2007007133001 Re Legent Clearing LLC (Dec. 5, 2008), *available at*: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=19048>.

[32] See, Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative (Nov. 2003), *available at*: [http://www.fincen.gov/statutes\\_regs/files/sarnarrcompletguidfinal\\_112003.pdf](http://www.fincen.gov/statutes_regs/files/sarnarrcompletguidfinal_112003.pdf).

[33] See, e.g., NML Risk Assessment at pages 81-82, *available at*: <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>.

[34] See, e.g., In the matter of Oppenheimer & Co. Inc., Exchange Act Release No. 74141 (Jan. 27, 2015), *available at*: <http://www.sec.gov/litigation/admin/2015/33-9711.pdf> (settled matter); In the matter of Gilford Securities, Incorporated, Exchange Act Release No. 65450 (Sept. 30, 2011), *available at* <https://www.sec.gov/litigation/admin/2011/33-9264.pdf> (settled matter); In the matter of Ronald S. Bloomfield, Robert Gorgia, and John Earl Martin, Sr, Exchange Act Release No. 71632 (Feb. 27, 2014), *available at* <http://www.sec.gov/litigation/opinions/2014/33-9553.pdf>; In the matter of Ferris, Baker Watts, Inc., Exchange Act Release No. 59372 (Feb. 10, 2009), *available at*: <https://www.sec.gov/litigation/admin/2009/34-59372.pdf> (settled matter).

[35] ational Exam Program Risk Alert: Broker-Dealer Controls Regarding Customer Sales of Micro-Cap Securities (October 9, 2014), *available at*: <http://www.sec.gov/about/offices/ocie/broker-dealer-controls-microcap-securities.pdf>.

[36] *Available at*: <http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf>.



[37] See, e.g., In the matter of Pinnacle Capital Markets LLC, Exchange Act Release No. 62811 (Sept. 1, 2010), available at <http://www.sec.gov/litigation/admin/2010/34-62811.pdf> (settled matter); In the matter of Hold Brothers On-Line Investment Services, LLC, Exchange Act Release No. 67924 (Sept. 25, 2012), available at <http://www.sec.gov/litigation/admin/2012/34-67924.pdf> (settled matter).

[38] In the matter of Wedbush Securities Inc., Exchange Act Release No. 73652 (Nov. 20, 2014) (settled action), available at <http://www.sec.gov/litigation/admin/2014/34-73652.pdf>. See, also, FINRA's complaint against Wedbush Securities, FINRA Department of Market Regulation and Department of Enforcement v. Wedbush Securities Inc., Disciplinary Proceeding No. 20090206344-01 (August 18, 2014), available at: <http://disciplinaryactions.finra.org/viewdocument.aspx?DocNB=37085>.

[39] National Exam Risk Alert on Master/Sub-accounts (Sept. 29, 2011), available at: <http://www.sec.gov/about/offices/ocie/riskalert-mastersubaccounts.pdf>. See, also, NML Risk Assessment at pages 78-81, available at: <http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%932006-12-2015.pdf>.

[40] Broker-dealers are required to report suspicious transactions that are “conducted or attempted by, at, or through a broker-dealer”, among other criteria. 31 C.F.R. 1023.320. As such, any limitation based on classification of a “customer” is not consistent with the rule.

[41] See, e.g., Letter of Acceptance, Waiver and Consent No. 2013035821401 re Brown Brothers Harriman & Co. (Feb. 4, 2014), available at: <http://www.finra.org/web/groups/industry/@ip/@enf/@ad/documents/industry/p443448.pdf>, for the proposition that to be reasonably designed, an AML program must take into account the services offered to customers. See, also, Letter of Acceptance, Waiver and Consent No. 2013035109701 re: LPL Financial LLC (May 6, 2015), available at: <http://disciplinaryactions.finra.org/Search/ViewDocument/48016>.

*Modified: June 18, 2015*

# 2021 Report on FINRA's Examination and Risk Monitoring Program

INTRODUCTION	1
FIRM OPERATIONS	5
Anti-Money Laundering	5
Cybersecurity and Technology Governance	8
Outside Business Activities and Private Securities Transactions	11
Books and Records	13
Regulatory Events Reporting	14
Fixed Income Mark-up Disclosure	16
COMMUNICATIONS AND SALES	18
Reg BI and Form CRS	18
Communications with the Public	19
Private Placements	24
Variable Annuities	26
MARKET INTEGRITY	30
CAT	30
Best Execution	31
Large Trader Reporting	33
Market Access	35
Vendor Display Rule	36
FINANCIAL MANAGEMENT	38
Net Capital	38
Liquidity Management	40
Credit Risk Management	41
Segregation of Assets and Customer Protection	43
APPENDIX—USING FINRA REPORTS IN YOUR FIRM'S COMPLIANCE PROGRAM	45

## Introduction

This Report on FINRA's Risk Monitoring and Examination Activities (the Report) is designed to inform member firms' compliance programs by providing annual insights from FINRA's ongoing regulatory operations. For selected regulatory obligations, the Report: (1) identifies the applicable rule and key related considerations for member firm compliance programs; (2) summarizes noteworthy findings from recent examinations and outlines effective practices that FINRA observed during its oversight; and (3) provides additional resources that may be helpful to member firms.

The Report replaces two of FINRA's prior publications: (1) the Report on FINRA Examination Findings and Observations, which provided an analysis of prior examination results; and (2) the Risk Monitoring and Examination Priorities Letter, which highlighted areas we planned to review in the coming year.

FINRA expects to revisit the Report annually, as we did with these prior publications. Many of the areas addressed in the Report represent ongoing core compliance responsibilities that are reviewed as part of our risk-based exam program each year. Where applicable, we will continue to evolve the information in these areas to address changes in business models, technologies, compliance practices and other factors that may affect how regulatory obligations are fulfilled. Other areas addressed in the Report may be episodic or tied to a particular development, such as a new regulatory requirement or investment product. We expect to include these areas during the periods when they may be most relevant for member firms' compliance programs.

FINRA welcomes feedback on how we can improve future publications of this Report. Please contact Ursula Clay, Senior Vice President, Member Supervision at (646) 315-7375 or by [email](#); or Elena Schlickemaier, Senior Principal Analyst, Member Supervision, at (202) 728-6920 or by [email](#).

### Firms' Practices During COVID-19

In *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), we shared common themes FINRA noted through discussions with firms about the steps they reported taking in response to the pandemic and in connection with their move to remote work environments. This Report does not address exam findings, observations or effective practices specifically relating to how firms adjusted their operations during the pandemic. Those reviews are underway now and will be addressed in a future publication.

## Selected Highlights

This Report addresses several regulatory key topics for each of the four categories: (1) Firm Operations; (2) Communications and Sales; (3) Market Integrity; and (4) Financial Management. As described further in the “How to Use This Report” section below, the importance and relevance of the considerations, findings and effective practices in each of these areas will vary for each member firm.

In general, however, there are several key areas to highlight that impact compliance programs across a large population of member firms:

- ▶ **Regulation Best Interest (Reg BI) and Form CRS** – We will continue to focus on assessing whether member firms have established and implemented policies, procedures, and a system of supervision reasonably designed to comply with Reg BI and Form CRS. However, in 2021, we intend to expand the scope of our Reg BI and Form CRS reviews and testing to effect a more comprehensive review of firm processes, practices and conduct. As always, FINRA will take appropriate action in the event we observe conduct that may cause customer harm, would have violated previous standards (*e.g.*, suitability), or indicates a clear disregard of the requirements of Reg BI and Form CRS. In the Reg BI and Form CRS section below, member firms should review considerations our staff will use when examining a firm for compliance with Reg BI and Form CRS. The Report also includes a list of previously published considerations and materials—such as our [Reg BI Topic Page](#).
- ▶ **Consolidated Audit Trail (CAT)** – As we noted in *Regulatory Notice 20-31* (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT), all member firms that receive or originate orders in National Market System (NMS) stocks, over-the-counter (OTC) equity securities or listed options must report to CAT. All proprietary trading activity, including market making activity, is subject to CAT reporting. There are no exclusions or exemptions for size or type of firm or type of trading activity. FINRA is in the early stages of reviewing for compliance with certain CAT obligations; accordingly, exam findings or effective practices are not included in this Report but will be provided later when more information is available. In the interim, member firms should review the list of recommended steps provided in the *Notice* and the list of considerations and relevant resources provided in this Report in assessing the adequacy of their CAT compliance programs.
- ▶ **Cybersecurity** – Member firms’ ongoing and increasing reliance on technology for many customer-facing activities, communications, trading, operations, back-office and compliance programs—especially in our current remote work environment—requires them to address new and existing cybersecurity risks, including risks relating to cybersecurity-enabled fraud and crime. A firm’s cybersecurity program should be reasonably designed and tailored to the firm’s risk profile, business model and scale of operations. FINRA reminds firms that we review cybersecurity programs for compliance with business continuity plan requirements, as well as the SEC’s Regulation S-P Rule 30, which requires member firms to have policies and procedures addressing the protection of customer records and information. Given the increase in remote work and virtual client interactions, combined with an increase in cyber-related crimes, we encourage member firms to review the considerations, observations and effective practices noted in the Report, as well as *Regulatory Notice 20-13* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic), [Report on Selected Cybersecurity Practices – 2018](#) and [Report on Cybersecurity Practices – 2015](#).
- ▶ **Communications with the Public** – FINRA continues to evaluate member firms for compliance with FINRA Rule [2210](#) (Communications with the Public), which includes principles-based content standards that are designed to apply to ongoing developments in communications technology and practices. In addition, we are increasingly focused on communications relating to certain new products, and how member firms supervise, comply with recordkeeping obligations, and address risks relating to new digital communication channels. This focus includes risks associated with app-based platforms with interactive or “game-like” features that are intended to influence customers, their related forms of marketing, and the appropriateness of the activity that they are approving clients to undertake through those platforms (*e.g.*, under FINRA Rule [2360](#) (Options)). The Report also addresses the communications relating to cash management services that sweep customer cash into affiliate or partner



banks or money market funds (Cash Management Accounts). As always, we remain focused on reviewing member firms' communications relating to complex products, as well as the information firms convey to senior and vulnerable investors.

- ▶ **Best Execution** – FINRA has routinely reviewed member firms for their compliance with best execution obligations under FINRA Rule [5310](#) (Best Execution and Interpositioning) in our examinations. Among other things, FINRA has continued to focus on potential conflicts of interest in order-routing decisions, appropriate policies and procedures for different order and security types, and the sufficiency of member firms' reviews of execution quality. We also conducted a [targeted review](#) of member firms that do not charge commissions for customer transactions ("zero commission" trading) to evaluate the impact that not charging commissions has or will have on member firms' order-routing practices and decisions, and other aspects of member firms' business. In addition to general compliance considerations, findings and effective practices from our examination program, the Report also includes themes we noted in the "zero commission" targeted review.
- ▶ **Variable Annuities** – FINRA continues to evaluate variable annuity exchanges under FINRA Rule [2330](#) (Members' Responsibilities Regarding Deferred Variable Annuities) and, when applicable, under Reg BI. Additionally, in early 2020, we engaged in an informal review of buyout written supervisory procedures (WSPs), training, and disclosures for member firms whose customers were impacted by a recent announcement from an insurer with sizable variable annuity assets stating it will terminate servicing agreements, cancel certain trail commissions for registered representatives, and provide buyout offers to its variable annuity customers. In addition to reviewing considerations and findings provided in the Report, we encourage member firms to consider the effective practices we identified as part of this particular review.

## How to Use the Report

FINRA's Risk Monitoring and Examination Programs evaluate member firms for compliance with relevant obligations and consider specific risks relating to each firm, including those relating to a firm's business model, supervisory control system and prior exam findings, among other considerations. While the topics addressed in this Report are selected for their interest to the largest number of member firms, they may include areas that are not relevant to an individual member firm and omit other areas that are applicable.

FINRA advises each member firm to review the Report and consider incorporating relevant practices into its compliance programs in a manner tailored to its activities. The Report is intended to be just one of the tools a member firm can use to help inform the development and operation of its compliance program; it does not represent a complete inventory of regulatory obligations, compliance considerations, examination findings, effective practices or topics that FINRA will examine.

FINRA also reminds member firms to stay apprised of new or amended laws, rules and regulations, and to update their WSPs and compliance programs on an ongoing basis, as new regulatory obligations may be part of future examinations. FINRA encourages member firms to reach out to their designated Risk Monitoring Analyst if they have any questions about the considerations, findings and effective practices described in this Report.

Each area of regulatory obligations is set forth as follows:

- ▶ **Regulatory Obligations and Related Considerations** – A brief description of:
  - relevant federal securities laws, regulations and FINRA rules; and
  - questions FINRA may ask or consider when examining your firm for compliance with such obligations. We encourage member firms to use these questions, if applicable, when evaluating their compliance programs and related controls, and preparing for FINRA examinations.

### ► Exam Findings and Effective Practices

- Noteworthy findings that FINRA has noted at some—but not all—member firms, including:
  - new findings from recent examinations;
  - findings we highlighted in the [2017](#), [2018](#) and [2019](#) Exam Findings Reports, and continue to note in recent examinations;
  - in certain sections, topics noted as “Emerging Risks” representing potentially concerning practices that FINRA has observed and which may receive increased scrutiny going forward; and
  - for certain topics, such as Cybersecurity, Liquidity Management and Credit Risk, observations that suggested improvements to a firm’s control environment to address potential weaknesses that elevate risk, but for which there are not specific rule violations.
- Select effective practices FINRA observed in recent exams, as well as those we noted in prior Exam Findings Reports and which we continue to see, that may help member firms, depending on their business model, evaluate their own programs.

## Supervision

We do not address supervisory deficiencies or practices in a separate Supervision topic, but rather, address them as part of the underlying regulatory obligation (*e.g.*, supervisory shortcomings relating to annuity exchanges are addressed in the Variable Annuities section).

## Senior and Vulnerable Investors

We also do not include a separate section on senior or vulnerable investors because FINRA considers such investors when evaluating firms’ compliance programs for many of the topics addressed in this Report, including determining the egregiousness of an exam finding or rule violation. FINRA remains highly focused on, and committed to, protecting senior and vulnerable investors, and takes this into consideration when evaluating communications, recommendations of certain products, and sales practice conduct.

### ► Additional Resources – A list of relevant FINRA Notices, other reports, tools and online resources.

The Report also includes an Appendix that outlines how member firms have used similar FINRA reports (Exam Findings Reports or Priorities Letters) in their compliance programs.

As a reminder, the Report—like our previous Exam Findings Reports and Priorities Letters—does not create any new legal or regulatory requirements or new interpretations of existing requirements. You should not infer that FINRA requires member firms to implement any specific practices described in this report extend beyond the requirements of existing federal securities rules and regulations or FINRA rules.

# Firm Operations

## Anti-Money Laundering

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

The Bank Secrecy Act (BSA) requires firms to monitor for, detect and report suspicious activity conducted or attempted by, at, or through the firms to the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN). Firms should also be aware of the recently enacted Anti-Money Laundering Act of 2020, which may result in material revisions to the implementing regulations over time.

FINRA Rule [3310](#) (Anti-Money Laundering Compliance Program) requires that members develop and implement a written anti-money laundering (AML) program reasonably designed to comply with the requirements of the BSA and its implementing regulations. Additionally, FinCEN's Customer Due Diligence (CDD) rule requires that firms identify beneficial owners of legal entity customers, understand the nature and purpose of customer accounts, and conduct ongoing monitoring of customer accounts to identify and report suspicious transactions and—on a risk basis—update customer information.

#### Related Considerations

- ▶ How does your firm's AML compliance program address new business lines, products, customers and risks?
- ▶ Does your firm tailor and adequately resource their AML program to the firm's business model and associated AML risks?
- ▶ Does your firm's independent testing confirm that it maintains appropriate risk-based procedures for collecting and verifying customer identification information on all individuals and entities that would be considered customers under the Customer Identification Program rule, and beneficial owners of legal entity customers under the CDD rule?
- ▶ Does your firm review the integrity of its data feeds for its surveillance and monitoring programs?
- ▶ How does your firm coordinate with your clearing firm, including with respect to the filing of joint suspicious activity reports?
- ▶ Does your firm document the results of its reviews and investigations into potentially suspicious activity identified by exception reports?

### Exam Findings and Effective Practices

#### Exam Findings

- ▶ **Inadequate AML Transaction Monitoring** – Not tailoring transaction monitoring to address firms' business risk(s).
- ▶ **Limited Scope for Suspicious Activity Reports (SARs)** – Not requiring staff to notify AML departments or file SARs for a range of events involving suspicious transactions, such as financial crime-related events, including but not limited to cybersecurity events, account compromises, account takeovers, new account fraud and fraudulent wires.

- ▶ **Inadequate AML Framework for Cash Management Accounts** – Failing to incorporate, or account for, in their AML programs, the AML risks relating to Cash Management Accounts, including the following:
  - monitoring, investigating and reporting suspicious money movements;
  - a list of red flags in their WSPs indicative of potentially suspicious transactions; or
  - expanding or enhancing their AML compliance program resources to address Cash Management Accounts.
- ▶ **Unclear Delegation of AML Responsibilities** – Non-AML staff (*e.g.*, business line staff responsible for trade surveillance) failing to escalate suspicious activity monitoring alerts to AML departments because firms did not: (1) clearly define the activities that were being delegated; (2) articulate those delegations and related surveillance responsibilities in their WSPs; or (3) train non-AML staff on AML surveillance policies and procedures.
- ▶ **Data Integrity Gaps** – Excluding certain types of data and customer accounts from monitoring programs as a result of problems with ingesting certain data, inaccuracies and missing information in data feeds.
- ▶ **Failure to Document Investigations** – Not documenting initial reviews and investigations into potentially suspicious activities identified by SARs.
- ▶ **Concerns About High-Risk Trading by Foreign Legal Entity Accounts** – Inadequate identification of or follow-up on increased trading by foreign legal entity accounts in similar low-float and low-priced securities, which raised concerns about potential ownership or control by similar beneficial owners.
- ▶ **Insufficient Independent Testing** – Not reviewing how the firm's AML program was implemented; not ensuring independence of the testing; and not completing tests on an annual calendar year basis.
- ▶ **Improper Reliance on Clearing Firms** – Introducing firms relying primarily or entirely on their clearing firms for transaction monitoring and suspicious activity reporting, even though they are required to monitor for suspicious activity attempted or conducted through their firms.

## Emerging AML and Other Financial Crime Risks

### Microcap and Other Fraud

Some firms continue to engage in fraud, financial crimes and other problematic practices, such as those described in the [SEC Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities](#), which addresses microcap and penny stock activity transacted in omnibus accounts maintained for foreign financial institutions and foreign affiliates of U.S. broker-dealers.

### Issuers Based in Restricted Markets

Certain foreign national and foreign entity nominee accounts appear to have been opened solely to invest in the initial public offerings and subsequent aftermarket trading in one or more exchange-listed issuers based in restricted markets, such as China. FINRA has observed red flags that the owners of the accounts may be acting at the direction of others, multiple accounts being opened using the same foreign bank for the source of funds or multiple accounts with the same employer and same email domain. The trading activity may include multiple similar limit orders being placed by the accounts at the same time, which could be indicative of coordinated and manipulative trading of the issuers' securities.

### Risks Relating to Special Purpose Acquisition Companies (SPACs)

Some firms are engaging in the formation and initial public offerings (IPOs) of SPACs without having adequate WSPs that would require independently conducting due diligence of SPACs' sponsors, and procedures that address other potential fraud risks, including but not limited to:

- ▶ misrepresentations and omissions in offerings documents and communications with shareholders regarding SPAC acquisition targets, such as the prospects of the target company and its financial condition;
- ▶ fees associated with SPAC transactions, including cash and non-cash compensation and compensation earned by affiliates;
- ▶ control of funds raised in SPAC offerings; and
- ▶ insider trading (where underwriters and SPAC sponsors may possess and trade around material non-public information regarding potential SPAC acquisition targets, including private placement offerings with rights of first refusal provided to certain investors prior to the acquisition).

## Effective Practices

- ▶ **Customer Identification Program** – Using, on a risk-basis, both documentary (such as drivers' licenses or passports) and non-documentary methods (such as using third-party sources) to verify customers' identities.
- ▶ **Monitoring for Fraud During Account Opening** – Implementing additional precautions during account opening, including limiting automated approval of multiple accounts opened by a single customer; reviewing account application fields for repetition or commonalities among multiple applications; and using technology to detect indicators of automated scripted attacks in the digital account application process.
- ▶ **Bank Account Verification, Restrictions on Fund Transfers and Ongoing Monitoring** – Confirming customers' identities through verbal confirmation, following client verification protocols or using a third-party verification service, such as Early Warning System (EWS); monitoring of outbound money movement requests post-ACH set-up; restricting fund transfers in certain situations; and conducting ongoing monitoring of accounts.
- ▶ **Collaboration With Clearing Firms** – Understanding the allocation of responsibilities between clearing and introducing firms for handling ACH transactions; and implementing policies and procedures to comply with those responsibilities.

- ▶ **AML Compliance Tests** – Confirming annual AML independent tests evaluate the adequacy of firms’ AML compliance programs, review firms’ SAR reporting processes, and include sampling and transaction testing of firms’ monitoring programs.
- ▶ **Risk Assessments** – Updating risk assessments based on the results of AML independent tests, audits, and changes in size or risk profile of the firms, including their businesses, registered representatives and customer account types; and using AML risk assessments to inform the focus of firms’ independent AML tests.
- ▶ **Testing of Transaction Monitoring and Model Validation** – Performing regular, ongoing testing and tuning of transaction monitoring models, scenarios and thresholds; and confirming the integrity of transaction monitoring data feeds and validating models (which are more frequently used at large firms).
- ▶ **Collaboration with AML Department** – Increasing the likelihood that all potentially reportable events are referred to the AML department by establishing a line of communication (such as reporting and escalation processes, awareness and educational programs, regular meetings, policies and procedures, or exception reports) between the AML department and other departments that may observe potentially reportable events (such as registered representatives and client-facing teams, technology, cybersecurity, compliance, operations, trading desks and fraud departments).
- ▶ **Training Programs** – Designing training programs for each of the roles and responsibilities of the AML department (as well as departments that regularly work with AML) and addressing all AML regulatory and industry developments.

## Additional Resources

- ▶ *Regulatory Notice [20-13](#)* (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- ▶ *Regulatory Notice [19-18](#)* (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations)
- ▶ [SEC Staff Bulletin: Risks Associated with Omnibus Accounts Transacting in Low-Priced Securities](#)
- ▶ [Anti-Money Laundering \(AML\) Template for Small Firms](#)
- ▶ [Frequently Asked Questions \(FAQ\) Regarding Anti-Money Laundering \(AML\)](#)
- ▶ [Anti-Money Laundering \(AML\) Topic Page](#)

## Cybersecurity and Technology Governance

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

The SEC’s Regulation S-P Rule 30 requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information. FINRA Rule [4370](#) (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members’ operations. In addition to firms’ compliance with SEC regulations, FINRA reminds firms that cybersecurity remains one of the principal operational risks facing broker-dealers, and expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

Technology-related problems, such as problems in firms’ change- and problem-management practices, can expose firms to operational failures that may compromise firms’ ability to comply with a range of rules and regulations, including FINRA Rules [4370](#) (Business Continuity Plans and Emergency Contact Information), [3110](#) (Supervision) and [4511](#) (General Requirements), as well as Securities Exchange Act of 1934 (Exchange Act) Rules 17a-3 and 17a-4.

## Related Considerations

- ▶ What kind of governance structure has your firm developed to identify and respond to cybersecurity risks?
- ▶ What is the scope of your firm's Data Loss Prevention program, including encryption controls?
- ▶ How does your firm address branch-specific cybersecurity risks?
- ▶ What kind of training does your firm conduct on cybersecurity, including phishing?
- ▶ What process does your firm have to evaluate your firm's vendors' cybersecurity controls?
- ▶ Has your firm implemented multi-factor authentication (MFA) or other relevant access management controls?
- ▶ What controls does your firm implement to mitigate system capacity performance and integrity issues that may undermine its ability to conduct business and operations, monitor risk or report key information?
- ▶ How does your firm document system change requests and approvals?
- ▶ What type of testing does your firm perform prior to changes being moved into a production environment and post-implementation?
- ▶ What are your firm's procedures for tracking information technology problems and their remediation? Does your firm categorize problems based on their business impact?

## Exam Observations and Effective Practices

### Exam Observations

- ▶ **Data Loss Prevention Programs** – Not encrypting all confidential data, including a broad range of non-public customer information in addition to Social Security numbers (such as other account profile information and firm information).
- ▶ **Branch Policies, Controls and Inspections** – Not maintaining branch-level written cybersecurity policies; inventories of branch-level data, software and hardware assets; and branch-level inspection and automated monitoring programs.
- ▶ **Training** – Not providing comprehensive training to registered representatives, personnel, third-party providers and consultants on cybersecurity risks relevant to individuals' roles and responsibilities, including phishing.
- ▶ **Vendor Controls** – Not implementing and documenting formal policies and procedures to review prospective and existing vendors' cybersecurity controls and managing the lifecycle of firms' engagement with all vendors (*i.e.*, from onboarding, to ongoing monitoring, through off-boarding, including defining how vendors will dispose of non-public client information).
- ▶ **Access Management** – Not implementing access controls, including developing a "policy of least privilege" to grant system and data access only when required and removing it when no longer needed; not limiting and tracking individuals with administrator access; and not implementing MFA for registered representatives, employees, vendors and contractors.
- ▶ **Inadequate Change Management Supervision** – Insufficient supervisory oversight for application and technology changes (including upgrades, modifications to or integration of firm or vendor systems), which lead to violations of other regulatory obligations, such as those relating to data integrity, cybersecurity, books and records, and confirmations.
- ▶ **Limited Testing and System Capacity** – Order management system, account access and trading algorithm malfunctions due to a lack of testing for changes or system capacity issues.



## Emerging Cybersecurity Risks

FINRA recently observed increased numbers of cybersecurity- or technology-related incidents at firms, including:

- ▶ systemwide outages;
- ▶ email and account takeovers;
- ▶ fraudulent wire requests;
- ▶ imposter websites; and
- ▶ ransomware.

We also noted data breaches at some firms and remain concerned about increased risks for firms that do not implement practices to address phishing emails or require MFA for accessing non-public information.

We remind firms to review the practices noted below, as well as the materials noted in the associated Additional Resources section.

## Effective Practices

- ▶ **Insider Threat and Risk Management** – Collaborating across technology, risk, compliance, fraud, and internal investigations/conduct departments to assess key risk areas, monitor access and entitlements, and investigate potential violations of firm rules or policies with regard to data access or data accumulation.
- ▶ **Incident Response Planning** – Establishing and regularly testing written formal incident response plans that outlined procedures for responding to cybersecurity and information security incidents; and developing frameworks to identify, classify, prioritize, track and close cybersecurity-related incidents.
- ▶ **System Patching** – Implementing timely application of system security patches to critical firm resources (*e.g.*, servers, network routers, desktops, laptops and software systems) to protect non-public client or firm information.
- ▶ **Asset Inventory** – Creating and keeping current an inventory of critical information technology assets—including hardware, software and data—as well as corresponding cybersecurity controls.
- ▶ **Change Management Processes** – Implementing change management procedures to document, review, prioritize, test, approve, and manage hardware and software changes, as well as system capacity, in order to protect non-public information and firm services.

## Additional Resources

- ▶ [Regulatory Notice 20-32](#) (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud)
- ▶ [Information Notice 03/26/20](#) (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19))
- ▶ [Regulatory Notice 20-13](#) (FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic)
- ▶ [Report on Selected Cybersecurity Practices – 2018](#)
- ▶ [Report on Cybersecurity Practices – 2015](#)
- ▶ [Small Firm Cybersecurity Checklist](#)
- ▶ [Core Cybersecurity Controls for Small Firms](#)
- ▶ [Customer Information Protection Topic Page](#)
- ▶ [Cybersecurity Topic Page](#)
- ▶ [Non-FINRA Cybersecurity Resources](#)



# Outside Business Activities and Private Securities Transactions

## Regulatory Obligations and Related Considerations

### Regulatory Obligations

FINRA Rules [3270](#) (Outside Business Activities of Registered Persons) and [3280](#) (Private Securities Transactions of an Associated Person) require registered representatives to notify their firms in writing of proposed outside business activities (OBAs), and all associated persons to notify their firms in writing of proposed private securities transactions (PSTs), so firms can determine whether to limit or allow those activities. A firm approving a PST where the associated person has or may receive selling compensation must record and supervise the transaction as if it were executed on behalf of the firm.

### Related Considerations

- ▶ Do your firm's WSPs explicitly state where notification or pre-approval is required to engage in an OBA or PST?
- ▶ Does your firm require associated persons or registered persons to complete and update, as needed, questionnaires and attestations regarding their involvement—or potential involvement—in OBAs and PSTs; and if yes, how often?
- ▶ Do you have a process in place in to update a registered representative's Form U4 with OBAs that meet the disclosure requirements of that form?
- ▶ What methods does your firm use to identify individuals involved in undisclosed OBAs and PSTs?
- ▶ Does your firm take into account the unique regulatory considerations and characteristics of digital assets when reviewing digital asset OBAs and PSTs?
- ▶ How does your firm supervise PSTs, including digital asset PSTs, and document its compliance with the supervisory obligations?
- ▶ Does your firm record the PSTs on its books and records, including PSTs involving new or unique products and services?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **Incorrect Interpretation of Requirements** – Interpreting “compensation” too narrowly (by focusing on only direct compensation, such as salary or commissions, rather than evaluating all direct and indirect financial benefits from PSTs, such as membership interests, receipt of preferred stock and tax benefits); and, as a result, erroneously determining that certain activities were not PSTs, or approving participation in proposed transactions without adequately considering whether the firms need to supervise the transaction as if it were executed on their own behalf.
- ▶ **No Documentation** – Not retaining the documentation necessary to demonstrate firms' compliance with the supervisory obligations for PSTs and not recording the transactions on the firm's books and records because certain PSTs were not consistent with firms' electronic systems (such as where securities businesses conducted by a registered representative would not be captured in their clearing firm's feed of purchases and sales activity).
- ▶ **No or Insufficient Notice and Notice Reviews** – Registered persons failing to notify their firms in writing of OBAs or PSTs; and WSPs not requiring the review of such notices, or the documentation that such reviews had taken place.

- ▶ **No PST Monitoring** – Not monitoring limitations placed on OBAs or PSTs, such as prohibiting registered representatives from soliciting firm clients to participate in the OBA or PST.
- ▶ **No Review and Recordkeeping of Digital Asset Activities** – Incorrectly assuming all digital assets are not securities and, therefore, not evaluating digital asset activities, including activities performed by affiliates, to determine whether they are PSTs; and for certain digital asset or other activities that were deemed to be PSTs because registered representatives received selling compensation, not supervising such activities or recording such transactions on the firm’s books and records.

## Emerging OBA/PST Risks

### Paycheck Protection Program (PPP) Loans for Registered Representatives

FINRA noted that some registered representatives received a PPP loan for an OBA that had not been disclosed to their firms, and which may have required an update to their Form U4 as well. Firms should consider reviewing the publicly available data on PPP loans to determine if they have a registered representative who obtained a PPP loan for an undisclosed OBA.

## Effective Practices

- ▶ **Questionnaires** – Requiring registered representatives and other associated persons to complete upon hire, and periodically thereafter, detailed, open-ended questionnaires with regular attestations regarding their involvement—or potential involvement—in new or previously disclosed OBAs and PSTs (including asking questions relating to any other businesses where they are owners or employees; whether they are raising money for any outside activity; whether they act as “finders”; and any expected revenues or other payments they receive from any entities other than member firms, including affiliates).
- ▶ **Thorough Reviews** – Conducting reviews to learn about all OBAs and PSTs at the time of a registered representative’s initial disclosure to the firm and periodically thereafter, including thorough reviews of:
  - social media, professional networking and other publicly available websites and other sources (such as legal research databases and court records);
  - email, social media and other communications;
  - interviews with registered representatives; and
  - documentation supporting the activity (such as organizational documents).
- ▶ **Monitoring** – Monitoring significant changes in or other red flags relating to registered representatives’ or associated persons’ performance, production levels, or lifestyle that may indicate involvement in undisclosed or prohibited OBAs and PSTs (or other business or financial arrangements with their customers, such as borrowing or lending), including conducting regular, periodic background checks and reviews of:
  - correspondence (including social media);
  - fund movements;
  - marketing materials;
  - online activities;
  - customer complaints; and
  - financial records (including bank statements and tax returns).

- ▶ **Affiliate Activities** – Considering whether registered representatives’ and other associated persons’ activities with affiliates, especially self-offerings, may implicate FINRA Rules 3270 and 3280.
- ▶ **WSPs** – Clearly identifying types of activities or investments that would constitute an OBA or PST subject to disclosure/approval or not, as well as defining compensation, and in some cases, providing FAQs to remind employees of scenarios that they might not otherwise consider applicable to these rules.
- ▶ **Training** – Conducting training on OBAs and PSTs during onboarding and periodically thereafter, including regular reminders that registered representatives must give written notice of such activities to their firms and update their disclosures.
- ▶ **Disciplinary Action** – Imposing significant consequences—including heightened supervision, fines or termination—for registered representatives and associated persons who fail to notify firms in writing and receive approval for their OBAs and PSTs.
- ▶ **Digital Asset Checklists** – Creating checklists with a list of considerations to confirm whether digital asset activities would be considered OBAs or PSTs (including reviewing private placement memoranda or other materials and analyzing the underlying products and investment vehicle structures).

## Additional Resources

- ▶ *Regulatory Notice [20-23](#)* (FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- ▶ *Regulatory Notice [18-08](#)* (FINRA Requests Comment on Proposed New Rule Governing Outside Business Activities and Private Securities Transactions)
- ▶ *Notice to Members [96-33](#)* (NASD Clarifies Rules Governing RRs/IAs)
- ▶ *Notice to Members [94-44](#)* (Board Approves Clarification on Applicability of Article III, Section 40 of Rules of Fair Practice to Investment Advisory Activities of Registered Representatives)

## Books and Records

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

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) require a firm to, among other things, create and preserve, in an easily accessible place, originals of all communications received and sent relating to its “business as such.”

Such records must be immediately produced or reproduced and may be maintained and preserved for the required time on electronic storage media (ESM) subject to the conditions set forth in Exchange Act Rule 17a-4(f)(2) (ESM Standards), including “non-rewriteable and non-erasable format.” Firms must also provide notification to FINRA as required by Exchange Act Rule 17a-4(f)(2)(i), including a representation that the selected storage media 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).

## Related Considerations

- ▶ What kind of vendors, such as cloud service providers (Cloud Vendors), does your firm use to comply with Books and Records Rule requirements, including storing required records on ESM? How does it confirm compliance with the Books and Records Rules, ESM Standards and ESM Notification Requirements?
- ▶ Has your firm reviewed its Books and Records Rule policies and procedures to confirm they address all vendors, including Cloud Vendors?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **Misinterpreted Obligations** – Not performing due diligence to verify vendors’ ability to comply with Books and Records Rules requirements if they use that vendor; or not confirming that service contracts and agreements comply with ESM Notification Requirements, because they did not understand that all required records must comply with the Books and Records Rules, including records stored using Cloud Vendors’ storage services.
- ▶ **No ESM Notification** – Not complying with the ESM Notification Requirements, including obtaining the third-party attestation letters required by Exchange Act Rule 17a-4(f)(3)(vii).

### Effective Practices

- ▶ **Contract Review** – Reviewing vendors’ contracts and agreements to assess whether firms will be able to comply with the Books and Records Rules, ESM Standards and ESM Notification Requirements.
- ▶ **Testing and Verification** – Testing all vendors’—including Cloud Vendors’—capabilities to fulfill regulatory obligations by, for example, simulating a regulator’s examinations by requesting records, and engaging regulatory or compliance consultants to confirm compliance with the Books and Records Rule, ESM Standards and ESM Notification Requirements (and, in some cases, engaging the consultant to provide the third-party attestation).
- ▶ **Attestation Verification** – Confirming with vendors, including Cloud Vendors, whether the firms or the vendors will provide the third-party attestation.

## Additional Resources

- ▶ [Frequently Asked Questions about the Amendments to Broker/Dealer Books and Records Rules Under the Securities Exchange Act of 1934](#)
- ▶ [Books and Records Requirements Checklist](#)
- ▶ [Books and Records Topic Page](#)

# Regulatory Events Reporting

## Regulatory Obligations and Related Considerations

### Regulatory Obligations

FINRA Rule [4530](#) (Reporting Requirements) requires firms to promptly report to FINRA, and associated persons to promptly report to firms, specified events, including, for example, violations of securities laws and FINRA rules, certain written customer complaints and certain disciplinary actions taken by the firm. Firms must also report quarterly to FINRA statistical and summary information regarding certain written customer complaints.

## Related Considerations

- ▶ Do your firm's WSPs require associated persons to report written customer complaints, judgments, liens and other events to the firm's compliance department?
- ▶ Does your firm provide periodic reminders or training on such requirements, and what consequences does your firm impose on those persons that do not comply?
- ▶ How does your firm monitor for red flags of unreported written customer complaints and other reportable events?
- ▶ How does your firm ensure that it accurately and timely reports to FINRA written customer complaints that associated persons reported to your firm's compliance department?
- ▶ How does your firm determine the problem and product codes it uses for its statistical reporting of written customer complaints to FINRA?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **No Reporting to the Firm** – Associated persons not reporting complaints, judgments, liens and other events to the firms' compliance departments because they were not aware of firm requirements;
- ▶ **Inadequate Surveillance** – Firms not conducting regular email and other surveillance for unreported events.
- ▶ **No Reporting to FINRA** – Failing to report to FINRA written customer complaints that associated persons reported to the firms' compliance departments.
- ▶ **Incorrect Rule 4530 Product/Problem Codes** – As part of the statistical reporting to FINRA, failing to use codes that correlated to the most prominent product or the most egregious problem alleged in the written customer complaints, but instead, reporting less prominent or severe codes or other codes based on the firms' investigations or other information.

### Effective Practices

- ▶ **Compliance Questionnaires** – Developing detailed annual compliance questionnaires to verify the accuracy of associated persons' disclosures, including follow-up questions (such as whether they have ever filed for bankruptcy, have any pending lawsuits, are subject to an unsatisfied judgments or liens, or received any written customer complaints).
- ▶ **Email Surveillance** – Conducting email surveillance targeted to identify unreported complaints (by, for example, including complaint-related words in their keyword lexicons, reviewing for unknown email addresses, and conducting random email checks).
- ▶ **Review of Registered Representatives' Financial Condition** – Identifying expenses, settlements and other payments that may indicate unreported events by conducting periodic reviews of their associated persons' financial condition, including background checks and credit reports.
- ▶ **Review of Publicly Available Information** – Conducting periodic searches of associated persons' names on web forums, court filings and other publicly available databases, including reviewing for any judgments, liens and other reportable events.

## Additional Resources

- ▶ *Regulatory Notice [20-17](#)* (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- ▶ *Regulatory Notice [20-02](#)* (FINRA Requests Comment on the Effectiveness and Efficiency of Its Reporting Requirements Rule)
- ▶ *Regulatory Notice [15-05](#)* (SEC Approves Consolidated FINRA Rule Regarding Background Checks on Registration Applicants)
- ▶ *Regulatory Notice [13-08](#)* (FINRA Amends Rule 4530 to Eliminate Duplicative Reporting and Provide the Option to File Required Documents Online Using a New Form)
- ▶ FINRA's [Rule 4530 Reporting Requirements](#)
- ▶ FINRA's [Rule 4530 Reporting Codes](#)
- ▶ [FINRA Report Center](#) – 4530 Disclosure Timeliness Report Card

## Fixed Income Mark-up Disclosure

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

Since 2018, FINRA's and the Municipal Securities Rulemaking Board's (MSRB) amendments to FINRA Rule [2232](#) (Customer Confirmations) and MSRB Rule [G-15](#) have required firms to provide additional transaction-related information to retail customers for certain trades in corporate, agency and municipal debt securities (other than municipal fund securities). Disclosed mark-ups and mark-downs must be expressed as both a total dollar amount for the transaction and a percentage of prevailing market price (PMP). In addition, for all retail customer trades in corporate, agency and municipal debt securities (other than municipal fund securities), firms must disclose on the confirmation the time of execution and a security-specific link to the FINRA or MSRB website where additional information about the transaction is available, along with a brief description of the information available on the website.

#### Related Considerations

- ▶ What are the frequency, scope and depth of your firm's review of the accuracy of your firm's confirmations, and does it include reviewing samples of confirmations?
- ▶ How does your firm work with its clearing firm(s) to ensure the accuracy of your firm's confirmations?
- ▶ Is the process to ensure mark-up disclosures appear on confirmations manual or automated?
- ▶ What is the scope of diligence and oversight your firm conducts on customer confirmation vendors?
- ▶ Has your firm considered how to maintain consistent and correct disclosures for fixed income transactions executed across different vendors, platforms or trading desks?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **Incorrect PMP Determinations** – Adjusting the PMP in firms’ order entry systems to subtract registered representatives’ concession or sales credit from the mark-up; PMP not presumptively relying on the dealer’s contemporaneous cost or proceeds; deciding that firms’ costs or proceeds were no longer “contemporaneous” without sufficient evidence as required by FINRA Rule 2121.02(b)(4) and using other pricing information to determine the PMP.
- ▶ **Incorrect Compensation Disclosures** – Disclosing additional charges separately from disclosed mark-ups or mark-downs, even when such charges reflected firm compensation; disclosing registered representatives’ sales credits or concessions as separate line items on confirmations, in addition to the mark-up or mark-down, without clear and accurate labeling; inaccurately labeling only the sales credits or concessions portion as the total mark-up or mark-down.
- ▶ **Failure to Provide Accurate Time of Execution** – Disclosing times of execution on customer confirmations that did not match the times of execution disseminated by the Electronic Municipal Market Access system (EMMA) or Trade Reporting and Compliance Engine (TRACE).
- ▶ **Disclosure for Structured Notes** – Failing to provide disclosures on customer confirmations for trades in TRACE-reportable structured notes because firms did not realize the notes were subject to FINRA Rule 2232 or did not receive the PMP from the structured note distributors.
- ▶ **Incorrect Designation of Institutional Accounts** – Failing to provide disclosures to certain customers because the firm identified those customers’ accounts as “institutional,” even though the customers did not meet the “institutional” definition in FINRA Rule [4512\(c\)](#) (Customer Account Information) or MSRB Rule G-8(a)(xi).

### Effective Practices

- ▶ **Confirmation Review** – Performing regular reviews of confirmations, including samples of confirmations, to confirm the accuracy of all disclosures, including all of the required disclosure elements, including the mark-up or mark-down, the time of execution and the security-specific link (with CUSIP).
- ▶ **Collaborating With Clearing Firms** – For correspondent firms, engaging with clearing firms to understand their policies and processes for providing mark-up disclosure.
- ▶ **Due Diligence of Vendors** – Conducting due diligence into customer confirmation vendors’ processes and methodology to determine PMP.
- ▶ **Product and Customer Review** – Reviewing firm confirmation systems and processes to confirm that they cover all products and customers subject to FINRA Rule 2232 (in particular, whether they accurately categorize “institutional” customers using the definition in FINRA Rule 4512(c) or MSRB Rule G-8(a)(xi)).

## Additional Resources

- ▶ *Regulatory Notice 17-24* (FINRA Issues Guidance on the Enhanced Confirmation Disclosure Requirements in Rule 2232 for Corporate and Agency Debt Securities)
- ▶ [Report Center](#) – FINRA’s MSRB Markup/Markdown Analysis Report
- ▶ [Report Center](#) – FINRA’s TRACE Markup/Markdown Analysis Report
- ▶ [Fixed Income Confirmation Disclosure: Frequently Asked Questions \(FAQ\)](#)
- ▶ [Municipal Securities Topic Page](#)
- ▶ [Fixed Income Topic Page](#)



# Communications and Sales

## Reg BI and Form CRS

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

[Reg BI](#) establishes a “best interest” standard of conduct for broker-dealers and associated persons when they make a recommendation to retail customers of any securities transaction or investment strategy involving securities, including recommendations of types of accounts.

Broker-dealers are also required to provide a brief relationship summary, [Form CRS](#), to retail investors on the types of client and customer relationship and services the firm offers; the fees, costs, conflicts of interest, and required standard of conduct associated with those relationships and services; whether the firm and its financial professionals currently have reportable legal or disciplinary history; and how to obtain additional information about the firm.

#### Related Considerations

- ▶ Does your firm have policies, procedures and controls in place to assess recommendations using a best interest standard?
- ▶ Do your firm and your associated persons apply a best interest standard to recommendations of types of accounts and recommendations to roll over or transfer assets from one type of account to another?
- ▶ Do your firm’s policies, procedures and controls continue to address compliance with FINRA Rule [2111](#) (Suitability), which still applies to recommendations made to non-retail investors?
- ▶ Does your firm have policies, procedures and controls addressing Reg BI’s recordkeeping requirements?
- ▶ Has your firm provided adequate Reg BI training to its sales and supervisory staff?
- ▶ Do your firm and your associated persons consider the express new elements of care, skill and costs when making recommendations to retail customers?
- ▶ Do your firm and your associated persons consider reasonably available alternatives to the recommendation?
- ▶ Do your firm and your registered representatives guard against excessive trading, irrespective of whether the broker-dealer or associated person “controls” the account?
- ▶ Does your firm have policies and procedures to provide the disclosures required by Reg BI?
- ▶ Does the firm place any material limitations on the securities or investment strategies involving securities that may be recommended to a retail customer, and if so, does the firm address and disclose such limitations?
- ▶ Does your firm have policies and procedures to identify and address conflicts of interest?
- ▶ If the firm is not dually registered as an investment adviser, commodity advisor or municipal advisor, does the firm or any of its associated persons who are not dually registered advisors or advisory representatives use “adviser” or “advisor” in their name or title?
- ▶ Does your firm have policies, procedures and controls in place regarding the filing, updating and delivery of Form CRS?
- ▶ Does your firm’s Form CRS accurately respond to the disciplinary history question with regard to the firm and its financial professionals?
- ▶ If your firm has a website, has it posted its Form CRS in a prominent location on that website?
- ▶ Does your firm’s Form CRS include required conversation starters, headers and prescribed language?



## Exam Findings and Effective Practices

As FINRA is in the early stages of reviewing for compliance with these new obligations, this Report will not include exam findings or effective practices relating to Reg BI and Form CRS. FINRA notes that the SEC held a virtual [Roundtable on Regulation Best Interest and Form CRS](#) that discussed some early examination findings. We anticipate issuing a separate publication in the future after more exams have been conducted. FINRA reminds firms to review the materials noted in the Additional Resources section below.

## Additional Resources

- ▶ [Regulatory Notice 20-18](#) (FINRA Amends Its Suitability, Non-Cash Compensation and Capital Acquisition Broker (CAB) Rules in Response to Regulation Best Interest)
- ▶ [Regulatory Notice 20-17](#) (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- ▶ [FINRA Highlights Firm Practices from Regulation Best Interest Preparedness Reviews](#)
- ▶ [SEC's Regulation Best Interest, Form CRS and Related Interpretations](#)
- ▶ FINRA's [Regulation Best Interest \(Reg BI\) Topic Page](#)

## Communications with the Public

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

FINRA Rule [2210](#) (Communications with the Public) categorizes all communications into three categories—correspondence, retail communications or institutional communications—and sets principles-based content standards that are designed to apply to ongoing developments in communications technology and practices. The rule also includes standards for firms' approval, review and recordkeeping procedures, as well as requirements to file certain communications with FINRA. FINRA Rule 2210 requires, among other things, that all communications be based on principles of fair dealing and good faith, be fair and balanced, provide a sound basis for evaluating the facts "in regard to any particular security or type of security, industry, or service" and include all "material fact[s] or qualification[s]" necessary to ensure such communications are not misleading. In addition, the rule prohibits false, misleading, promissory or exaggerated statements or claims, and projections of performance.

#### Related Considerations

##### ▶ General Standards

- Do your firm's communications include material information necessary to make them fair, balanced and not misleading? For example, if a communication promotes the benefits of a high-risk or illiquid security, does it explain the associated risks?
- Do your firm's communications balance specific claims of investment benefits from a securities product or service (especially complex products) with the key risks specific to that product or service?
- Do your firm's communications contain false, misleading or promissory statements or claims?
- Do your firm's communications contain predictions or projections of investment performance to investors that are generally prohibited by FINRA Rule 2210(d)(1)(F)?

► **Digital Communication Channels**

- Does your firm’s digital communication policy address all permitted and prohibited digital communication channels and features available to your customers and associated persons?
- Does your firm review for red flags that may indicate a registered representative is communicating through unapproved communication channels, and does your firm follow up on such red flags? For example, red flags might include email chains that copy unapproved representative email addresses, references in emails to communications that occurred outside approved firm channels, or customer complaints mentioning such communications.
- How does your firm supervise and maintain books and records in accordance with SEC and FINRA rules for all approved digital communications?
- If your firm offers an app to customers that includes an interactive element, does the information provided to customers constitute a “recommendation” that would be covered by Reg BI, which requires a broker-dealer to act in a retail customer’s “best interest,” or suitability obligations under FINRA Rule [2360](#) (Options)? If so, how does your firm comply with these obligations?
- If your firm’s app platform design includes “game-like” aspects that are intended to influence customers to engage in certain trading or other activities, how does your firm address and disclose the associated potential risks to your customers?
- Do your firm’s communications—regardless of the platform through which they are made—comply with the content standards set forth in FINRA Rule 2210?

► **Digital Asset Communications** – If your firm or an affiliate engages in digital asset activities:

- Does your firm provide a fair and balanced presentation in marketing materials and retail communications, including addressing risks presented by digital asset investments, and not misrepresenting the extent to which digital assets are regulated by FINRA or the federal securities laws or eligible for protections thereunder, such as Securities Investor Protection Corporation (SIPC) coverage?
- Do your firm’s communications misleadingly imply that digital asset services offered through an affiliated entity are offered through and under the supervision, clearance and custody of a registered broker-dealer?

► **Cash Management Accounts Communications** – If your firm offers Cash Management Accounts, does it:

- Clearly communicate the terms of the Cash Management Accounts?
- Disclose that the Cash Management Accounts’ deposits are obligations of the destination bank, and not cash balances held by your firm?
- Confirm that its communications do not state or imply that:
  - brokerage accounts are similar to, or the same, as bank “checking and savings accounts” or other accounts insured by the Federal Deposit Insurance Corporation (FDIC); and
  - FDIC insurance coverage applies to funds when held at or by a registered broker-dealer?
- Review whether communications fairly explain the:
  - nature and structure of the program;
  - relationship of the brokerage accounts to any partner banks in the Cash Management Accounts;
  - amount of time it may take for customer funds to reach the bank accounts; and
  - risks of participating in such programs?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **Deficient Digital Assets Communications** – Failing to balance promotional statements with prominent risk disclosures; including false, misleading or unwarranted statements; using the same firm names, websites and other materials for broker-dealers and their digital asset affiliates; not identifying the (non-broker-dealer) entities responsible for digital asset offerings; and implying that digital assets were offered by the broker-dealer.
- ▶ **Misrepresentations in Cash Management Accounts Communications** – Misrepresenting material information relating to Cash Management Accounts in online and other communications (in some cases, despite written and verbal warnings from FINRA’s Advertising Regulation Department), including, for example, the firms’ status as broker-dealers rather than banks; the status of Cash Management Accounts as “checking and savings accounts;” the amount of FDIC insurance coverage for the deposits; the amount of time it may take for customer funds to reach the bank accounts; terms of the Cash Management Accounts; and risks of participating in such programs.
- ▶ **Insufficient Supervision and Recordkeeping for Digital Communication** – Not maintaining policies and procedures to reasonably identify and respond to red flags—such as customer complaints, representatives’ email, OBA reviews or advertising reviews—that registered representatives used impermissible business-related digital communications methods, including texting, messaging, social media, collaboration apps or “electronic sales seminars” in chatrooms.
- ▶ **No WSPs and Controls for Communication That Use Non-Member or OBA Names (so-called “Doing Business As” or “DBA” Names)** – Not maintaining WSPs to identify the broker-dealer clearly and prominently as the entity through which securities were offered in firm communications, such as websites, social media posts, seminars or emails that promote or discuss the broker-dealer’s securities business and identify a non-member entity, such as a representative’s OBA; and not including a “readily apparent reference” and hyperlink to FINRA’s BrokerCheck in such communications.

## Emerging Digital Communication Risks

### New Digital Platforms With Interactive and “Game-Like” Features

2020 witnessed a surge in new retail investors entering the markets via online brokers, as well as an increase in certain types of trading, including options. Some online broker-dealers’ apps—as well as those offered by other financial services and consumer-oriented businesses—include interactive and “game-like” features, as well as related forms of advertising and marketing. Such features affect many aspects of how firms interact and communicate with customers, from initial advertisements through the opening of accounts, recommendations and the presentation of different investment choices.

While such features may improve customers’ access to firm systems and investment products, they may also result in increased risks to customers if not designed with the appropriate compliance considerations in mind. Firms must evaluate these features to determine whether they meet regulatory obligations to:

- ▶ comply with any Reg BI and Form CRS requirements if any communications constitute a “recommendation” that requires a broker-dealer to act in a retail customer’s “best interest”;
- ▶ make disclosures relating to risks to customers, fees, costs, conflicts of interest, and required standards of conduct associated with the firm’s relationships and services;
- ▶ prohibit the use of false, exaggerated or misleading statements or claims in any communications and ensure all firm communications are fair and balanced and do not omit material information concerning products or services;
- ▶ comply with account opening requirements that require firms to gather information about customers (such as FINRA Rule [4512](#) (Customer Account Information)) and approve certain types of accounts, including options accounts (such as FINRA Rule [2360\(b\)\(16\)](#) (Diligence in Opening Accounts) and other supervisory controls relating to options, such as surveilling for optionsrelated customer complaints, excessive commissions and fees, and large amounts of losses);
- ▶ develop a comprehensive supervisory system for such communication methods, including surveilling for red flags of potential violative behavior and maintaining books and records of all communications related to the firm’s business as such; and
- ▶ address compliance with FINRA communications rules, such as FINRA Rules [2210](#) (Communications with the Public); [2211](#) (Communications with the Public About Variable Life Insurance and Variable Annuities); [2212](#) (Use of Investment Company Rankings in Retail Communications); [2213](#) (Requirements for the Use of Bond Mutual Fund Volatility Ratings); [2214](#) (Requirements for Use of Investment Analysis Tools); [2215](#) (Communications with the Public Regarding Securities Futures); [2216](#) (Communications with the Public Regarding Collateralized Mortgage Obligations) and [2220](#) (Options Communications).

## Effective Practices

- ▶ **Comprehensive Procedures for Digital Communications** – Maintaining and implementing procedures for firm digital communication channel policies, including:
  - **Monitoring of New Tools and Features** – Marketing, compliance and information technology departments working closely together, as well as with third-party vendors, to monitor new communication channels, apps and features available to their associated persons and customers.
  - **Defining and Enforcing What is Permissible and Prohibited** – Clearly defining permissible and prohibited digital communication channels, and blocking prohibited channels, tools or features, including those that prevent firms from complying with their recordkeeping requirements.
  - **Supervision** – Implementing supervisory review procedures tailored to each digital channel, tool and feature.
  - **Video Content Protocols** – Developing WSPs and controls for live-streamed public appearances, scripted presentations or video blogs.
  - **Training** – Implementing mandatory training programs prior to providing access to firm-approved digital channels, including expectations for business and personal digital communications and guidance for using all permitted features of each channel.
  - **Disciplinary Action** – Temporarily suspending or permanently blocking from certain digital channels or features those registered representatives who did not comply with the policies and requiring additional digital communications training.
- ▶ **Digital Asset Communications** – Maintaining and implementing procedures for firm digital asset communications, including:
  - **Risk Disclosure** – Prominently describing the risks associated with digital assets, including that such investments are speculative, involve a high degree of risk, are generally illiquid, may have no value, have limited regulatory certainty, are subject to potential market manipulation risks and may expose investors to loss of principal.
  - **Communication Review** – Reviewing firms' communications to confirm that they were not exaggerating the potential benefits of digital assets or overstating the current or future status of digital asset projects or platforms.
  - **Communication to Differentiate Digital Assets From Broker-Dealer Products** – Identifying, segregating and differentiating firms' broker-dealer products and services from those offered by affiliates or third parties, including digital asset affiliates; and clearly and prominently identifying entities responsible for non-securities digital assets businesses (and explaining that such services were not offered by the broker-dealer or subject to the same regulatory protections as those available for securities).
- ▶ **Reviews of Firms' Capabilities for Cash Management Accounts** – Requiring new product groups or departments to conduct an additional review for proposed Cash Management Accounts to confirm that the firms' existing business processes, supervisory systems and compliance programs—especially those relating to communications—can support such programs.
- ▶ **Use of Non-Member or OBA Names (so-called DBAs)** – Maintaining and implementing procedures for OBA names, including:
  - **Training** – Providing training on relevant FINRA rules and firm policies, and requiring annual attestations to demonstrate compliance with such requirements.
  - **Templates** – Requiring use of firm-approved vendors to create content or standardized templates populated with approved content and disclosures for all OBA communications (including websites, social media, digital content or other communications) that also concern the broker-dealer's securities business.

- **Prior Approval** – Prohibiting the use of OBA communications that concern the broker-dealer’s securities business without prior approval by compliance, and creating a centralized system for the review and approval of such communications, including content and disclosures.
- **Notification and Monitoring** – Requiring registered representatives to notify compliance of any changes to approved communications, and conducting periodic, at least annual, monitoring and review of previously approved communications for changes and updates.

## Additional Resources

- ▶ *Regulatory Notice [20-23](#)* (FINRA Encourages Firms to Notify FINRA if They Engage in Activities Related to Digital Assets)
- ▶ *Regulatory Notice [20-21](#)* (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- ▶ *Regulatory Notice [19-31](#)* (Disclosure Innovations in Advertising and Other Communications with the Public)
- ▶ *Regulatory Notice [17-18](#)* (Guidance on Social Networking Websites and Business Communications)
- ▶ *Regulatory Notice [11-39](#)* (Social Media Websites and the Use of Personal Devices for Business Communications)
- ▶ *Regulatory Notice [10-06](#)* (Guidance on Blogs and Social Networking Web Sites)
- ▶ [Advertising Regulation Topic Page](#)
- ▶ [Social Media Topic Page](#)

## Private Placements

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

As noted in *Regulatory Notice [10-22](#)* (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings), as part of their obligations under FINRA Rule [2111](#) (Suitability) and supervisory requirements under FINRA Rule [3110](#) (Supervision), firms must conduct a “reasonable investigation” by evaluating “the issuer and its management; the business prospects of the issuer; the assets held by or to be acquired by the issuer; the claims being made; and the intended use of proceeds of the offering.” The SEC’s Reg BI became effective on June 30, 2020, and would apply to recommendations of private offerings to retail customers. Reg BI similarly requires, among other things, a broker-dealer to exercise reasonable diligence, care and skill to understand the potential risks, rewards and costs associated with a private offering recommendation and have a reasonable basis to believe that the private offering recommendation could be in the best interest of at least some retail customers.

In addition, firms must make timely filings for specified private placement offerings with FINRA’s Corporate Financing Department under FINRA Rules [5122](#) (Private Placements of Securities Issued by Members) and [5123](#) (Private Placements of Securities).

#### Related Considerations

- ▶ What policies and procedures does your firm have to address filing requirements and timelines under FINRA Rules 5122 and 5123? How does it review for compliance with such policies?
- ▶ How does your firm use and evaluate consultants, experts or other third-party vendors’ due diligence reports?

- ▶ How does your firm conduct reasonable investigations on private placement offerings, including conducting further inquiry into red flags identified during the reasonable investigation process?
- ▶ How does your firm address conflicts of interest identified in third-party due diligence reports?
- ▶ How does your firm handle escrowed funds and amended terms in contingency offerings?
- ▶ If your firm is engaging in new business, such as Regulation A offerings or SPACs, has it implemented WSPs to address this business? If this business may constitute a material change in your firm's business operations, has your firm considered whether it needs to file a Continuing Membership Application (CMA)?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **Late Filings** – Not having policies and procedures, processes and supervisory programs to comply with filing requirements; and failing to make timely filings (with, in some cases, delays lasting as long as six to twelve months after the offering closing date).
- ▶ **No Reasonable Investigation** – Failing to perform reasonable investigations of private placement offerings prior to recommending the offerings to retail investors, including failing to conduct additional research about new offerings, relying on their experience with the same issuer in previous offerings and not conducting further inquiry into red flags identified during the investigation process.
- ▶ **Concerning Third-Party Due Diligence** – Failing to address red flags (such as disciplinary history of the issuer's management), conflicts of interest (such as undisclosed direct or indirect common ownership of affiliated entities or the issuer) or significant concerns (such as no legitimate operating history for the issuer) identified in third-party due diligence reports.

### Effective Practices

- ▶ **Private Placement Checklist** – Creating checklists with—or added to existing firm Regulation D and other offering checklists—all steps, filing dates, related documentation requirements and evidence of supervisory principal approval for the filing requirements of FINRA Rules 5122 and 5123.
- ▶ **Independent Research** – Conducting and documenting independent research on material aspects of the offering; identifying any red flags with the offering or the issuer (such as questionable business plans or unlikely projections or results); and addressing and, if possible, resolving concerns that would be relevant to a potential investor (such as tax considerations or liquidity restrictions).
- ▶ **Independent Verification** – Verifying information that was key to the performance of the offering (such as unrealistic costs projected to execute the business plan coupled with aggressively projected timing and overall rate of return for investors); and, in some cases, receiving support from due diligence firms, experts and third-party vendors.
- ▶ **Mitigating Conflicts of Interest** – Using firms' reasonable investigation processes to mitigate conflicts of interest and developing comprehensive disclosures for offerings involving firm affiliates or issuers whose control persons were also employed by the firm.
- ▶ **Ownership for Filings** – Assigning responsibility for private placement filing requirements to specific individual(s) or team(s) and conducting targeted, in-depth training about the firms' policies, process and technical filing requirements.
- ▶ **Automated Alert System** – Creating an automated system that alerts responsible individual(s) and supervisory principal(s) about upcoming and missed filing deadlines.



- ▶ **Private Placement Committee** – Creating a private placement committee (at larger firms) or formally designating one or more qualified persons (at smaller firms); charging committee-designated individuals with investigating and determining whether to approve the offering for sale to investors; and conducting research and identifying and highlighting red flags with the offering or the issuer.
- ▶ **Post-Approval Processes** – Using the investigation analysis to establish post-approval processes and investment limits based on the complexity or risk level of the offering.
- ▶ **Ongoing Monitoring** – Conducting ongoing monitoring after the offering to ascertain whether offering proceeds were used in a manner consistent with the offering memorandum, particularly for ongoing sales of an offering after initial closing.

## Additional Resources

- ▶ [Regulatory Notice 20-21](#) (FINRA Provides Guidance on Retail Communications Concerning Private Placement Offerings)
- ▶ [Regulatory Notice 10-22](#) (Obligations of Broker-Dealers to Conduct Reasonable Investigations in Regulation D Offerings)
- ▶ [Report Center – Corporate Financing Report Cards](#)
- ▶ [FAQs about Private Placements](#)
- ▶ [Corporate Financing Private Placement Filing System User Guide](#)
- ▶ [Private Placements Topic Page](#)

## Variable Annuities

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

FINRA Rule [2330](#) (Members' Responsibilities Regarding Deferred Variable Annuities) establishes sales practice standards regarding recommended purchases and exchanges of deferred variable annuities, including requiring a reasonable belief that the customer has been informed of the various features of annuities (such as surrender charges, potential tax penalties, various fees and costs, and market risk); and, prior to recommending the purchase or exchange of a deferred variable annuity, requiring reasonable efforts to determine the customer's age, annual income, investment experience, investment objectives, investment time horizon, existing assets and risk tolerance. To the extent that a broker-dealer or associated person is recommending a purchase or exchange of a deferred variable annuity to a retail customer, Reg BI's obligations, discussed above, also would apply.

In addition, the rule requires that firms conduct surveillance to determine if any associated person is effecting deferred variable annuity exchanges at a rate that might suggest conduct inconsistent with FINRA Rule 2330. Firms must also have procedures to implement corrective action to address any exchanges and conduct that violate FINRA Rule 2330.

#### Related Considerations

- ▶ How does your firm review for rates of variable annuity exchanges (*i.e.*, does your firm use any automated tools, exception reports or surveillance reports)?
- ▶ Does your firm have standardized review thresholds for rates of variable annuity exchanges?



- ▶ Does your firm have a process to confirm its variable annuity data integrity (including general product information, share class, riders and exchange-based activity) and engage with affiliate and non-affiliate insurance carriers to address inconsistencies in available data, data formats and reporting processes for variable annuities?
- ▶ What is your firm's process to supervise buyout offers (*i.e.*, does it include pre-approval, exception reports and post-transaction reviews)?
- ▶ What do your WSPs require registered representatives to do in order to support a determination that a transaction meets the standard of care requirements and that there is a reasonable basis for it? What is the manner in which they are to obtain, evaluate and record such information such as whether a customer would incur a surrender charge; would be subject to a new surrender period; would lose existing benefits; would be subject to increased fees or charges; would invest a substantial portion of the customer's liquid net worth in the variable annuity; has liquidity needs that are inconsistent with the variable annuity; would be investing in a share class that is not in the customer's best interest given his or her financial needs, time horizon and riders included with the contract; and has had another exchange within the preceding 36 months?
- ▶ Do your firm's policies and procedures require registered representatives to inform customers of the various features of annuities, such as surrender charges, potential tax penalties, various fees and costs, and market risk?
- ▶ How do your firm's registered principals supervise variable annuity transactions, including verifying how the customer would benefit from certain features of deferred variable annuities, such as tax-deferral, annuitization, or a death or living benefit? What processes, forms, documents and information do the firm's registered principals rely on to make such determinations?
- ▶ Does your firm have WSPs to address when it decides to stop selling or retires certain products, or opens buyout or exchange periods, including, but not limited to: how it will handle the product termination process; how it decides whether it offers an exchange or buyout; the scope of its exposure (in terms of contracts and customers); how it will notify customers and registered representatives; and how it will monitor for exchange rates?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **Not Addressing Buyouts** – Not addressing within firms' systems of supervision (by having applicable WSPs, delivering training, or making appropriate disclosures, etc.) that customers accepting buyouts may be losing valuable benefits associated with their existing products, subject to new surrender charge periods, and paying higher fees and expenses with new products (as was the case when customers were impacted by a recent announcement that an insurer with sizable variable annuity assets will terminate servicing agreements, cancel certain trail commissions for registered representatives, and provide buyout offers to its variable annuity customers).
- ▶ **Unsuitable Exchanges** – Not reasonably supervising recommendations of exchanges that were inconsistent with the customer's objectives and time horizon and resulted in, among other consequences, increased fees to the customer or the loss of material, paid-for accrued benefits.
- ▶ **Inadequate Source of Funds Review** – Not performing sufficient review of source of funds used to purchase new variable annuities.
- ▶ **Insufficient Training** – Not conducting training for registered representatives and supervisors regarding how to assess fees, surrender charges and long-term income riders to determine whether exchanges were suitable for customers.

## Effective Practices

### Buyout Offers

- ▶ **Policies and Reviews** – Performing a holistic review of buyout offers; requiring supervisory principal pre-approval (and, in some cases, additional second-level approval) for buyout offers; and requiring registered representatives' recommendations to consider all changes to customers' variable annuities, such as possible surrender charges, loss of benefits, contract values, riders, cash surrender values, expenses and fees.
- ▶ **Training** – Providing extensive, ongoing training and communications to all registered representatives about buyout offers and related compliance obligations (including, in some cases, creating dedicated firm telephone or chat helplines).
- ▶ **Conflicts of Interest** – Addressing and mitigating potential conflicts of interest for registered representatives who may recommend that customers pursue buyout offers to free up proceeds for new investments or variable annuity exchanges by, for example, leveling registered representatives' compensation for buyout offers, exchanges or new investments.
- ▶ **Additional Disclosures** – Developing new buyout offer disclosures or expanding existing variable annuity disclosure forms to address considerations for buyout offers.
- ▶ **Additional Post-Transaction Review** – Creating additional exception reports and conducting additional transaction monitoring for those customers who accepted buyout offers to confirm that those transactions were submitted for supervisory principal pre-approval (and, where required, additional second-level approval) and, if not, evaluating for compliance with FINRA Rule 2330.

### Exchanges

- ▶ **Automated Surveillance** – Using automated tools, exception reports and surveillance to review variable annuity exchanges, and implementing second-level supervision of supervisory reviews of exchange-related exception reports and account applications.
- ▶ **Rationales** – Requiring registered representatives to provide detailed written rationales for variable annuity exchanges for each customer (including confirming that such rationales address the specific circumstances for each customer and do not replicate rationales provided for other customers); and requiring supervisory principals to verify the information provided by registered representatives, including product fees, costs, rider benefits and existing product values.
- ▶ **Review Thresholds** – Standardizing review thresholds for rates of variable annuity exchanges; and monitoring for emerging trends across registered representatives, customers, products and branches.
- ▶ **Data Integrity** – Creating automated (rather than manual) solutions to synthesize variable annuity data (including general product information, share class, riders and exchange-based activity) and engaging with affiliated and non-affiliated insurance carriers to address inconsistencies in available data, data formats and reporting processes for variable annuities.

## Additional Resources

- ▶ *Regulatory Notice [20-18](#)* (FINRA Amends Its Suitability, Non-Cash Compensation and Capital Acquisition Broker (CAB) Rules in Response to Regulation Best Interest)
- ▶ *Regulatory Notice [20-17](#)* (FINRA Revises Rule 4530 Problem Codes for Reporting Customer Complaints and for Filing Documents Online)
- ▶ *Regulatory Notice [10-05](#)* (FINRA Reminds Firms of Their Responsibilities Under FINRA Rule 2330 for Recommended Purchases or Exchanges of Deferred Variable Annuities)

- ▶ *Notice to Members* [07-06](#) (Special Considerations When Supervising Recommendations of Newly Associated Registered Representatives to Replace Mutual Funds and Variable Products)
- ▶ *Notice to Members* [99-35](#) (The NASD Reminds Members of Their Responsibilities Regarding the Sales of Variable Annuities)
- ▶ [Variable Annuities Topic Page](#)
- ▶ [SEC's Regulation Best Interest, Form CRS and Related Interpretations](#)
- ▶ FINRA's [Regulation Best Interest \(Reg BI\) Topic Page](#)

# Market Integrity

## CAT

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

FINRA and the national securities exchanges have adopted rules requiring their members to comply with Exchange Act Rule 613 and the CAT NMS Plan FINRA Rule [6800 Series](#) (Consolidated Audit Trail Compliance Rule) (collectively, CAT Rules), which cover reporting to the CAT; clock synchronization; time stamps; connectivity and data transmission; development and testing; recordkeeping; the timeliness, accuracy and completeness of data; and compliance dates. *Regulatory Notice 20-31* (FINRA Reminds Firms of Their Supervisory Responsibilities Relating to CAT) describes certain practices and recommended steps firms should consider when developing and implementing their CAT Rules compliance program.

#### Related Considerations

- ▶ Do your firm's CAT Rules WSPs, at a minimum: (1) identify the individual, by name or title, responsible for the review of CAT reporting; (2) describe specifically what type of review(s) will be conducted of the data posted on the CAT Reporter Portal; (3) specify how often the review(s) will be conducted; and (4) describe how the review(s) will be evidenced?
- ▶ How does your firm confirm that the data reported by your firm or on your firm's behalf is transmitted in a timely fashion and is complete and accurate?
- ▶ How does your firm determine how and when clocks are synchronized, who is responsible for clock synchronization, how your firm evidences that clocks have been synchronized, and how the firm will self-report clock synchronization violations?
- ▶ Does your firm conduct daily reviews of the Industry Member CAT Reporter Portal (CAT Reporter Portal) to, among other requirements, review file status to ensure the file(s) sent by the member or by their reporting agent was accepted by CAT and to identify/address any file submission or integrity errors?
- ▶ Does your firm conduct periodic comparative reviews of accepted CAT data against order and trade records and the [CAT Reporting Technical Specifications](#)?
- ▶ Does your firm communicate regularly with your CAT reporting agent, review relevant CAT guidance and announcements, and report CAT reporting issues to the FINRA CAT Help Desk?

### Exam Findings and Effective Practices

As FINRA is in the early stages of reviewing for compliance with certain CAT Rules obligations, this Report does not include exam findings or effective practices relating to CAT Rules. FINRA reminds firms to review the materials noted in the Additional Resources section below.

#### Additional Resources

- ▶ *Regulatory Notice 19-19* (FINRA Reminds Firms to Register for CAT Reporting by June 27, 2019)
- ▶ *Regulatory Notice 17-09* (The National Securities Exchanges and FINRA Issue Joint Guidance on Clock Synchronization and Certification Requirements Under the CAT NMS Plan)
- ▶ [CAT NMS Plan](#)
- ▶ [Consolidated Audit Trail \(CAT\) Topic Page](#)

## Best Execution

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

FINRA Rule [5310](#) (Best Execution and Interpositioning) requires that, in any transaction for or with a customer or a customer of another broker-dealer, a member and persons associated with a member shall use reasonable diligence to ascertain the best market for the subject security, and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions. Firms must conduct a “regular and rigorous” review of the execution quality of customer orders if the firm does not conduct an order-by-order review. Where “regular and rigorous” reviews are used instead of order-by-order reviews, the reviews must be performed at a minimum on a quarterly basis and on a security-by-security, type-of-order basis (*e.g.*, limit order, market order and market on open order). If a firm identifies material differences in execution quality among the markets that trade the securities under review, it should modify its routing arrangements or justify why it is not doing so.

#### Related Considerations

- ▶ How does your firm determine whether to employ order-by-order or “regular and rigorous” reviews of execution quality?
- ▶ How does your firm implement and conduct an adequate “regular and rigorous” review of the quality of the executions of its customers’ orders?
- ▶ How does your firm document its “regular and rigorous” reviews, the data and other information considered, order routing decisions and the rationale used, and address any deficiencies?
- ▶ How does your firm address potential conflicts of interest in order-routing decisions, including those relating to its routing of orders to affiliated alternative trading systems (ATSs), affiliated broker-dealers, or affiliated exchange members? When routing orders to an affiliate, how does your firm ensure that its order-routing decisions are based upon best execution considerations and not unduly influenced by these affiliations?
- ▶ How does your firm address potential conflicts of interest in order-routing decisions, including those related to its routing of orders to market centers that provide payment for order flow (PFOF) or other-routing inducements?
- ▶ When routing to market centers that provide PFOF or other inducements, how does your firm ensure that its order-routing decisions are based upon best execution considerations and not unduly influenced by these economic incentives?
- ▶ If your firm engages in fixed income and options trading, has it established targeted controls to perform its best execution obligations for these products? Does your firm consider differences among security types within these products, such as the different characteristics and liquidity of U.S. Treasury securities compared to other fixed income securities?
- ▶ Does your firm perform its best execution obligations with respect to trading conducted in both regular and extended trading hours?
- ▶ Does your firm consider the risk of information leakage when assessing the execution quality of orders routed to a particular venue?
- ▶ What data sources does your firm use for its routing decisions and execution quality reviews for different order types and sizes, including odd lots?
- ▶ How does your firm handle fractional share investing in the context of its best execution obligations?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **No Assessment of Execution vs. Competing Markets** – Not comparing the quality of the execution obtained via firms’ existing order-routing and execution arrangements against the quality of execution they could have obtained from competing markets.
- ▶ **No Review of Certain Order Types** – Not conducting adequate reviews on a type-of-order basis, including, for example, on market, marketable limit or non-marketable limit orders.
- ▶ **No Evaluation of Required Factors** – Not considering certain factors set forth in FINRA Rule 5310 when conducting a “regular and rigorous review,” including, among other things, speed of execution, price improvement and the likelihood of execution of limit orders; and using routing logic that was not necessarily based on quality of execution.
- ▶ **Conflicts of Interest** – Not considering and addressing potential conflicts of interest relating to routing of orders to affiliated broker-dealers, ATSS or market centers that provide PFOF or other routing inducements, such as PFOF from wholesale market makers and exchange liquidity rebates.
- ▶ **Inadequate SEC Rule 606 Disclosures** – Not providing material disclosures in order-routing reports, such as the specific, material aspects of the non-directed order flow routed to firms’ trading desks, including that they stand to share in 100 percent of the profits generated by their trading as principal with their customers’ orders; material aspects of their relationships with each of the significant venues identified on their reports, including descriptions and terms of all arrangements for PFOF (including the amounts of PFOF on a per share or per order basis) and profit-sharing relationships that may have influenced the firms’ order routing decisions.

### Targeted Examination Letter on Zero Commissions

As part of FINRA’s ongoing 2020 [targeted review](#) of firms’ decisions to move to “zero-commission” trading, we are evaluating:

- ▶ whether the “zero-commission” model adversely affected firms’ compliance with their best execution obligations;
- ▶ how firms used other practices, such as Cash Management Accounts and PFOF, to potentially offset lost commission revenue; and
- ▶ whether firms prominently communicated restrictions and limitations of “zero-commission” structures and other fees charged to customers.

We will share the findings from this targeted review with member firms in a future publication once the review is complete.

## Effective Practices

- ▶ **Exception Reports** – Using exception reports and surveillance reports to support firms’ efforts to meet their best execution obligations.
- ▶ **PFOF Order Routing Impact Review** – Reviewing how PFOF affects the order-routing process, including the following factors: any explicit or implicit contractual arrangement to send order flow to a third-party broker-dealer; terms of these agreements; whether it is on a per share basis or per order basis; and whether it is based upon the type of order, size of order, type of customer or the market class of the security.
- ▶ **Risk-Based “Regular and Rigorous Reviews”** – Conducting “regular and rigorous” reviews, at a minimum, on a quarterly basis, but depending on the firm’s business model, conducting reviews more frequently than quarterly (such as monthly).
- ▶ **Continuous Updates** – Updating WSPs and best execution analysis to address account, market and technology changes.

## Additional Resources

- ▶ *Regulatory Notice 15-46* (Guidance on Best Execution Obligations in Equity, Options and Fixed Income Markets)
- ▶ *Notice to Members 01-22* (NASD Regulation Reiterates Member Firm Best Execution Obligations And Provides Guidance to Members Concerning Compliance)
- ▶ [Report Center, Equity Report Cards](#) – [FINRA’s Best Execution Outside-of-the-Inside Report Card](#)

# Large Trader Reporting

## Regulatory Obligations and Related Considerations

### Regulatory Obligations

Exchange Act Rule 13h-1 (Large Trader Rule) requires “large traders” to identify themselves as such to the SEC, disclose to other firms their large trader status and, in certain situations, comply with certain filing, recordkeeping and reporting requirements. These requirements help the SEC identify large traders and obtain trading information about their activity in the U.S. securities markets. In addition, broker-dealers will be required to obtain and report large trader information to the CAT for accounts with CAT Reportable Events.

### Related Considerations

- ▶ Has your firm created new WSPs or updated your WSPs to address the Large Trader Rule?
- ▶ Does the firm report its relevant proprietary trading activity with the designated Large Trader ID (LTID)?
- ▶ If not, how does your firm conduct daily calculations of its own trading activity to monitor its Large Trader status?
- ▶ Has your firm updated your new customer account process to address Large Trader Rule requirements?
- ▶ Does your firm perform daily calculations of customer accounts to determine if there were any new accounts that breached the daily or monthly thresholds?
- ▶ How does your firm notify customers of their regulatory obligations if the customer has been deemed to be an “Unidentified Large Trader”?
- ▶ How does your firm work with your clearing firm to comply with the Large Trader Rule?
- ▶ How is your firm preparing to comply with CAT reporting requirements relating to LTIDs?

## Exam Findings and Effective Practices

### Exam Findings

- ▶ **No WSPs** – Failing to update or create new WSPs to address the Large Trader Rule, including requirements for timely filing of [Form 13H](#) and identifying, monitoring, recordkeeping and filing for large traders and Unidentified Large Traders.
- ▶ **No Monitoring for Unidentified Large Traders** – Not monitoring customer activity to identify and detect Unidentified Large Traders and notifying such traders of their obligations.
- ▶ **Failure to Report LTID** – Not reporting the LTID on Electronic Blue Sheet (EBS) submissions for applicable orders.

### Effective Practices

- ▶ **WSPs** – Creating new or updated WSPs to address the Large Trader Rule, including developing WSPs to comply with the Large Trader Rule's recordkeeping requirements for its customer and proprietary trading businesses and Form 13H filing requirements for its proprietary business.
- ▶ **Form 13H Review** – Reviewing the accuracy of, and confirming any updates for, the firms' Form 13H.
- ▶ **Large Trader Check** – Adding a large trader check to firms' EBS policies and procedures to confirm that the LTID was populated and formatted correctly.
- ▶ **New Customer Account Process** – Requiring new institutional accounts to provide their LTID as part of the account opening process and, unless customers directed otherwise, requiring their LTIDs be applied to all of their new accounts.
- ▶ **Daily Large Trader and Customer Account Monitoring** – Completing daily large trader monitoring calculations to monitor the firms' large trader status; performing daily large trader monitoring calculations for their customer accounts to determine if there were any new accounts that breached the daily or monthly thresholds; and engaging their clearing firm to confirm that the clearing firm provided accurate customer LTID numbers and these numbers remained up to date.
- ▶ **Unidentified Large Traders** – Unless customers justified their exemption from the Large Trader Rule:
  - creating Unidentified Large Trader ID for those customers;
  - notifying them of potential registration obligations; and
  - advising them to request their LTID.

## Additional Resources

- ▶ U.S. Securities and Exchange Commission, Office of Compliance, Inspections and Examinations, [Observations from Examinations of Broker-Dealers and Investment Advisers: Large Trader Obligations](#) (Dec. 16, 2020)
- ▶ U.S. Securities and Exchange Commission, Division of Trading and Markets, [Responses to Frequently Asked Questions Concerning Large Trader Reporting](#) (Feb. 22, 2016)
- ▶ *Regulatory Notice 18-04* (FINRA and ISG Announce Extension of Effective Date for Certain Electronic Blue Sheet Data Elements and Updates to Certain Requestor and Exchange Codes)
- ▶ FINRA's [Frequently Asked Questions about Electronic Blue Sheets \(EBS\)](#)



## Market Access

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

Exchange Act Rule 15c3-5 (Market Access Rule) requires broker-dealers with market access or that provide market access to their customers to “appropriately control the risks associated with market access so as not to jeopardize their own financial condition, that of other market participants, the integrity of trading on the securities markets, and the stability of the financial system.”

#### Related Considerations

- ▶ If your firm has market access, or provides it, does it have reasonably designed risk-management controls and WSPs to manage the financial, regulatory or other risks associated with this business activity?
- ▶ If your firm is highly automated, how does it manage and deploy technology changes for systems associated with market access, and what controls does it use, such as kill switches, to monitor and respond to aberrant behavior by trading algorithms or other impactful marketwide events?
- ▶ How does your firm adjust credit limit thresholds for customers, including institutional customers (whether temporary or permanent)?
- ▶ Does your firm use any automated controls to timely revert *ad hoc* credit limit adjustments?
- ▶ If your firm uses third-party vendor tools to comply with its Market Access Rule obligations, does it review during vendor due diligence whether the vendor can meet the obligations of the rule, and how does your firm maintain direct and exclusive control of applicable thresholds?
- ▶ What type of training does your firm provide to individual traders regarding the steps and requirements for requesting *ad hoc* credit limit adjustments?
- ▶ Does your firm test your firm’s market access controls, including fixed income controls, and how do you use that test for your firm’s annual CEO certification attesting to your firm’s controls?

### Exam Findings and Effective Practices

#### Exam Findings

- ▶ **Insufficient Controls** – No pre-trade order limits, pre-set capital thresholds and duplicative and erroneous order controls for accessing ATSs, especially for fixed income transactions; unsubstantiated capital and credit pre-trade financial controls; no policies and procedures to govern intra-day changes to firms’ credit and capital thresholds, including requiring or obtaining approval prior to adjusting credit or capital thresholds, documenting justifications for any adjustments, and ensuring thresholds for temporary adjustments revert back to their pre-adjusted values.
- ▶ **Inadequate Financial Risk Management Controls** – For firms with market access, or those that provide it, inappropriate capital thresholds for trading desks, aggregate daily limits, or credit limits for institutional customers and counterparties.
- ▶ **Reliance on Vendors** – Relying on third-party vendors’ tools, including those of an ATS, to effect their financial controls, without understanding how vendors’ controls worked, and not maintaining direct and exclusive control over controls; and allowing the ATS to set capital thresholds for firms’ fixed income orders instead of establishing their own thresholds (some firms were not sure what their thresholds were, and had no means to monitor their usage during the trading day).

## Effective Practices

- ▶ **Pre-Trade Fixed Income Financial Controls** – Implementing systemic pre-trade “hard” blocks to prevent fixed income orders from reaching an ATS that would cause the breach of a threshold.
- ▶ **Intra-day (Ad Hoc) Adjustments** – Implementing processes for requesting, approving, reviewing and documenting ad hoc credit threshold increases, and returning the limits to their original values as needed.
- ▶ **Tailored Erroneous or Duplicative Order Controls** – Tailoring firms’ erroneous or duplicative order controls to particular products, situations or order types, and preventing the routing of a market order based on impact (Average Daily Volume Control) that are set at reasonably high levels (particularly in thinly traded securities); and calibrating to reflect, among other things, the characteristics of the relevant securities, the business of the firm, and market conditions.
- ▶ **Post-Trade Controls and Surveillance** – When providing direct market access via multiple systems, including sponsored access arrangements, employing reasonable controls to confirm that those systems’ records were aggregated and integrated in a timely manner and conducting holistic post-trade and supervisory reviews for, among other things, potential manipulative trading patterns.
- ▶ **Testing of Financial Controls** – Periodically testing their market access controls, which forms the basis for an annual CEO certification attesting to firms’ controls.

## Additional Resources

- ▶ *Regulatory Notice [16-21](#)* (SEC Approves Rule to Require Registration of Associated Persons Involved in the Design, Development or Significant Modification of Algorithmic Trading Strategies)
- ▶ *Regulatory Notice [15-09](#)* (Guidance on Effective Supervision and Control Practices for Firms Engaging in Algorithmic Trading Strategies)
- ▶ [Algorithmic Trading Topic Page](#)
- ▶ [Market Access Topic Page](#)

# Vendor Display Rule

## Regulatory Obligations and Related Considerations

### Regulatory Obligations

Rule 603 of Regulation NMS (Vendor Display Rule) generally requires broker-dealers to provide a consolidated display of market data for NMS stocks for which they provide quotation information to customers. Rule 600(b)(14) of Regulation NMS provides that the consolidated display includes “(i) the prices, sizes, and market identifications of the national best bid and national best offer for a security; and (ii) [c]onsolidated last sale information for a security,” while Rule 600(b)(15) of Regulation NMS provides that “consolidated last sale information” includes “the price, volume, and market identification of the most recent transaction report for a security that is disseminated pursuant to an effective national market system plan.”

### Related Considerations

- ▶ Which firm systems or platforms provide quotation information to customers?
- ▶ How does your firm monitor whether the current quotation information is distributed to customers?
- ▶ Does your firm make the quotation information available to customers when they are placing their orders?
- ▶ Does your firm review the quotation information received from the Securities Information Processor (SIP) or vendors to determine whether that information is in compliance with all the requirements of SEC Rule 603?

## Exam Findings and Effective Practices

### Exam Findings

#### ► Failure to Provide Consolidated Display

- **Missing Consolidated Display** – Failing to provide the entire consolidated display:
  - in all contexts and relevant stages in which a customer may make a trading or routing decision, (such as at point of order entry and order modification); and
  - across all platforms where customers may make a trading or routing decision (such as displaying all elements of the consolidated display on firms' web-based but not mobile device platforms).
- **Missing Elements** – Providing the consolidated display, but not including certain elements, such as:
  - national best bid and offer (NBBO) (while providing only the last sale information);
  - last sale information (while providing only the NBBO);
  - market identification for NBBO or last sale;
  - size associated with NBBO or last sale; and
  - real-time NBBO and last sale information (e.g., 15-minute delayed data).

#### ► Insufficient WSPs – Failing to maintain WSPs to address the Vendor Display Rule, periodic testing and validation that they were providing the consolidated display, and review for timely delivery of the consolidated display to customers (including evaluating and addressing any potential system latencies).

### Effective Practices

- **Confirming Market Data Feeds** – Confirming that firms received all market data feeds (including all exchanges) necessary to provide consolidated quote and last sale information to customers (including all prices, sizes and market identification data).
- **Customer Platform Reviews** – Performing a comprehensive review to confirm that firms provided the consolidated display to customers across all platforms where customers may make a trading or order-routing decision (including mobile platforms).
- **Latency Monitoring** – Monitoring for any delays or latency of the consolidated display, especially for mobile platforms, and then taking corrective action to confirm that the Consolidated Display information was current.
- **SIP Validation** – Performing periodic validation of quotation and last sale information against SIP data by creating screenshots of firms' quotation and last sale information for each customer platform and comparing it to SIP quotation and last sale information data.
- **Testing and Validation** – Testing and validating the consolidated display prior to and after upgrades or enhancements to customer platforms.

### Additional Resources

- [Regulatory Notice 15-52](#) (SEC Staff Provides Insight Into Firms' Obligations When Providing Stock Quote Information to Customers)
- [Regulation NMS Topic Page](#)

# Financial Management

## Net Capital

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

Exchange Act Rule 15c3-1 (Net Capital Rule) requires that firms must at all times have and maintain net capital at specific levels to protect customers and creditors from monetary losses that can occur when firms fail. Exchange Act Rule 17a-11 requires firms to notify FINRA in the event their net capital falls below the “minimum amount required” by the Net Capital Rule.

#### Related Considerations

- ▶ How does your firm review its net capital treatment of assets to confirm that they are correctly classified for net capital purposes?
- ▶ How does your firm confirm that it has correctly identified and aged all failed-to-deliver contracts, properly calculated the applicable net capital charges and correctly applied the deductions to its net capital calculation?
- ▶ For firms with expense sharing agreements, what kind of allocation methodology does your firm use and what kind of documentation does your firm maintain to substantiate its methodology for allocating specific broker-dealer costs to the firm or an affiliate?

### Exam Findings and Effective Practices

#### Exam Findings

- ▶ **Inaccurate Classification of Receivables, Liabilities and Revenue** – Incorrectly classifying receivables, liabilities and revenues, which resulted in inaccurate reporting of firms’ financial positions and, in some instances, a capital deficiency; incorrectly classifying non-allowable assets, such as large investments in certificates of deposit (CDs) because firms did not have a process to assess the net capital treatment of CDs pursuant to Exchange Act Rule 15c3-1(c)(2)(vi)(E); and not reviewing account agreements for CDs to determine whether they contained stipulations restricting withdrawals prior to maturity, including restricting their withdrawal or giving the bank discretion to permit or prohibit their withdrawal.
- ▶ **Failed to Deliver and Failed to Receive Contracts (Fails)** – Not having a process to correctly identify, track and age intra-month and end of the month Fails for firms’ operating an Exchange Act Rule 15a-6 chaperoning business, including:
  - **Inaccurate Net Capital Charge** – Failing to compute and apply the correct applicable net capital charge for aged Fails;
  - **No Information from Clearing Firm** – Failing to request or confirm receipt of timely information relating to Fails from their clearing firms;
  - **Gaps in Policies and Procedures** – Failing to address monitoring, reporting and aging of Fails in firms’ policies and procedures;
  - **Incorrect Balance Sheets and FOCUS Reports** – Failing to record Fails on firms’ balance sheet, and, as a result, filing incorrect FOCUS reports; and
  - **No Blotters** – Failing to maintain blotters for Fails.

- ▶ **Incorrect Capital Charges for Underwriting Commitments** – Not maintaining an adequate process to assess moment-to-moment and open contractual commitment capital charges on underwriting commitments, and not understanding their role as it pertained to the underwriting (*i.e.*, best efforts or firm commitment).
- ▶ **Inaccurate Recording of Revenue and Expenses** – Using cash accounting to record revenue and expenses as of the date the money changes hands, rather than accrual accounting (where firms would record revenue and expenses as of the date that revenue is earned or expenses are incurred); and making ledger entries as infrequently as once per month, as a result of which firms did not have adequate context to determine the proper accrual-based transaction date.
- ▶ **Insufficient Documentation Regarding Expense-Sharing Agreements** – Not delineating a method of allocation for payment; not allocating (fixed or variable) expenses proportionate to the benefit to the broker-dealer; or not maintaining sufficient documentation to substantiate firms' methodologies for allocating specific broker-dealer costs—such as technology fees, marketing charges, retirement account administrative fees and employees' compensation—to broker-dealers or affiliates.

### Effective Practices

- ▶ **Net Capital Assessment** – Performing an assessment of their net capital treatment of assets, including CDs, to confirm that they were correctly classified for net capital purposes.
- ▶ **Agreement Review** – Obtaining from, and verifying with, banks the withdrawal terms of any assets, with particular focus on CD products, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset's classification and its net capital charge for the terms of all assets, including CDs, and reviewing all of the agreement terms, focusing on whether withdrawal restrictions may affect an asset's classification and its net capital charge.
- ▶ **Training and Guidance** – Developing guidance and training for Financial and Operational Principal and other relevant staff on Net Capital Rule requirements for Fails, including how to report Fails on their balance sheets, track the age of Fails and, if necessary, calculate any net capital deficit resulting from aged Fails.
- ▶ **Aging Review** – Performing reviews to confirm that they correctly aged Fail contract charges and correctly applied a net capital deduction, when applicable, to their net capital calculation.
- ▶ **Collaboration with Clearing Firms** – Clarifying WSPs to address clearing firms' responsibilities regarding net capital requirements, including for Fails, and introducing firms engaging their clearing firms to confirm that:
  - introducing firms were receiving a record of all Fails on a daily basis (or at least monthly);
  - clearing firms' reports included all of the required information; and
  - introducing firms were correctly interpreting the clearing firms' reports (especially distinctions between trade date and settlement date and those dates' implications for aging calculations for Fails).

### Additional Resources

- ▶ [Interpretations of Financial and Operational Rules](#)
- ▶ [Regulatory Notice 15-33](#) (Guidance on Liquidity Risk Management Practices)
- ▶ [Regulatory Notice 10-57](#) (Funding and Liquidity Risk Management Practices)
- ▶ [Notice to Members 03-63](#) (SEC Issues Guidance on the Recording of Expenses and Liabilities by Broker/Dealers)
- ▶ [Funding and Liquidity Topic Page](#)

# Liquidity Management

## Regulatory Obligations and Related Considerations

### Regulatory Obligations

Effective liquidity controls are critical elements in a broker-dealer's risk management framework. Exchange Act Rule 17a-3(a)(23) requires firms that meet the thresholds specified under the rule to make and keep current records documenting the credit, market, and liquidity risk management controls established and maintained by the firm to assist it in analyzing and managing the risks associated with its business. FINRA routinely reviews firms' practices in these areas, and in *Regulatory Notice 15-33* (Guidance on Liquidity Risk Management Practices) shared observations on liquidity management practices.

### Related Considerations

- ▶ What departments at your firm are responsible for liquidity management?
- ▶ How often does your firm review and adjust its liquidity management plan and the stress test frameworks?
- ▶ Do your firm's liquidity management practices include steps to address specific stress conditions and identify firm staff responsible for addressing those conditions? Does your firm have a process for accessing liquidity during a stress event and determining how the funding would be used?
- ▶ Does your firm's contingency funding plan take into consideration the quality of collateral, term mismatches and potential counterparty losses of your firm's financing desks (in particular, in repo and stock loan transactions)?
- ▶ What kind of stress tests (e.g., market or idiosyncratic) does your firm conduct? Does your firm conduct stress tests in a manner and frequency that is appropriate for your firm's business model, for example tests limited to a single time horizon, or over multiple time horizons? Does your firm incorporate the results of those stress tests into your firm's business model?

## Exam Observations and Effective Practices

### Exam Observations

- ▶ **Not Extending the Stress Test Period** – Failing to expand stress tests from a single time horizon to multiple time horizons (such as 10 days to 30 days or longer).
- ▶ **Not Modifying Business Models** – Failing to incorporate the results of firms' stress tests into their business model.
- ▶ **No Liquidity Contingency Plans** – Failing to develop contingency plans for operating in a stressed environment with specific steps to address certain stress conditions, including identifying the firm staff responsible for enacting the plan, the process for accessing liquidity during a stress event and setting standards to determine how liquidity funding would be used.

### Effective Practices

- ▶ **Liquidity Risk Management Updates** – Updating liquidity risk management practices to take into account a firm's current business activities, including:
  - establishing governance around liquidity management, determining who is responsible for monitoring the firm's liquidity position, how often they monitor that position, and how frequently they meet as a group; and

- creating a liquidity management plan that considers:
  - quality of funding sources;
  - potential mismatches in duration between liquidity sources and uses;
  - potential losses of counterparties;
  - how the firm obtains funding in a business-as-usual (BAU) condition, and stressed conditions;
  - assumptions based on idiosyncratic and market-wide conditions; and
  - early warning indicators, and escalation procedures, if risk limits are breached.
- ▶ **Stress Tests** – Conducting stress tests in a manner and frequency that considered the firm’s business model, including:
  - assumptions specific to the firm’s business, and based on historical data;
  - the firm’s sources and uses of liquidity, and if sources could realistically fund its uses in a stressed environment;
  - the potential impact of off-balance sheet items on liquidity;
  - frequency of conducting stress tests, in accordance with the risk and complexity of the firm’s business; and
  - periodic review of stress test results by appropriate governance groups.

## Additional Resources

- ▶ *Regulatory Notice [15-33](#)* (Guidance on Liquidity Risk Management Practices)
- ▶ *Regulatory Notice [10-57](#)* (Funding and Liquidity Risk Management Practices)
- ▶ [Funding and Liquidity Topic Page](#)

# Credit Risk Management

## Regulatory Obligations and Related Considerations

### Regulatory Obligations

Under the financial responsibility rules, and related supervisory obligations, firms need to properly capture, measure, aggregate, manage and report credit risk, including risk exposures that may not be readily apparent. Such responsibility can be incurred under clearing arrangements, prime brokerage arrangements (especially fixed income prime brokerage), “give up” arrangements, sponsored access arrangements (discussed above in the Market Access section) or principal letters. Further, firms should maintain a robust internal control framework where they manage credit risk and they identify and address all relevant risks covering the extension of credit to their customers and counterparties. Weaknesses within the firm’s risk management and control processes could result in a firm incorrectly capturing its exposure to credit risk.

### Related Considerations

- ▶ Does your firm maintain a robust internal control framework to capture, measure, aggregate, manage, supervise and report credit risk?

- ▶ Does your firm review whether it is accurately capturing its credit risk exposure, maintain approval and documented processes for increases or other changes to assigned credit limits and monitor exposure to affiliated counterparties?
- ▶ Does your firm have a process to confirm it is managing the quality of collateral and monitoring for exposures that would have an impact on capital?

## Exam Observations and Effective Practices

### Exam Observations

- ▶ **No Credit Risk Management Reviews** – Not evaluating firms' risk management and control processes to confirm whether they were accurately capturing their exposure to credit risk.
- ▶ **No Credit Limit Assignments** – Not maintaining approval and documentation processes for assignment, increases or other changes to credit limits.
- ▶ **No Monitoring Exposure** – Not monitoring exposure to firms' affiliated counterparties.

### Effective Practices

- ▶ **Credit Risk Framework** – Developing comprehensive internal control frameworks to capture, measure, aggregate, manage and report credit risk, including:
  - establishing house margin requirements;
  - identifying and assessing credit exposures in real-time environments;
  - issuing margin calls and margin extensions (and resolving unmet margin calls);
  - establishing the frequency and manner of stress testing for collateral held for margin loans and secured financing transactions; and
  - having a governance process for approving new, material margin loans.
- ▶ **Credit Risk Limit Changes** – Maintaining approval and documentation processes for increases or other changes to assigned credit limits, including:
  - having processes for monitoring limits established at inception, and on an ongoing basis, for customers and counterparties;
  - reviewing how customers and counterparties adhere to these credit limits, and what happens if these credit limits are breached; and
  - maintaining a governance structure around credit limit approvals.
- ▶ **Counterparty Exposure** – Monitored exposure to their affiliated counterparties, considering their:
  - creditworthiness;
  - liquidity and net worth;
  - track record of past performance (*e.g.*, traded products, regulatory history, past arbitration and litigation); and
  - internal risk controls.

## Additional Resources

- ▶ [Funding and Liquidity Topic Page](#)



## Segregation of Assets and Customer Protection

### Regulatory Obligations and Related Considerations

#### Regulatory Obligations

Exchange Act Rule 15c3-3 (Customer Protection Rule) imposes certain requirements on firms that are designed to protect customer funds and securities. Firms are obligated to maintain custody of customer securities and safeguard customer cash by segregating these assets from the firm's proprietary business activities, and promptly deliver to their owner upon request. Firms can satisfy this requirement by either keeping customer funds and securities in their physical possession, or in a good control location that allows the firm to direct their movement (*e.g.*, a clearing corporation).

#### Related Considerations

- ▶ What is your firm's process to prevent, identify, research and escalate new or increased deficits which are in violation of the Customer Protection Rule?
- ▶ What controls does your firm have in place to identify and monitor its possession or control deficits, including the creation, cause and resolution?
- ▶ If your firm claims an exemption from the Customer Protection Rule and it is required to forward customer checks promptly to your firm's clearing firm, how does your firm implement consistent processes for check forwarding and maintain accurate blotters to demonstrate that checks were forwarded in a timely manner?
- ▶ How does your firm train staff on Customer Protection Rule requirements?
- ▶ What are your firm's processes to confirm that your firm correctly completes its reserve formula calculation and maintains the amounts that must be deposited into the special reserve bank account(s)?
- ▶ If your firm is engaging in digital asset transactions, what controls and procedures has it established to support facilitation of such transactions, including initial issuance or secondary market trading of digital assets? Has the firm analyzed these controls and procedures to address potential concerns that they may be viewed as a custodian (*i.e.*, holding or controlling customer property)?

### Exam Findings and Effective Practices

#### Exam Findings

- ▶ **Inconsistent Check-Forwarding Processes** – Not implementing consistent processes for check forwarding to comply with an exemption from the Customer Protection Rule.
- ▶ **Inaccurate Reserve Formula Calculations** – Failing to correctly complete reserve formula calculations due to errors in coding because of limited training and staff turnover, challenges with spreadsheet controls, limited coordination between various internal departments and gaps in reconciliation calculations.
- ▶ **Omitted or Inaccurate Blotter Information** – Maintaining blotters with insufficient information to demonstrate that checks were forwarded in a timely manner and inaccurate information about the status of checks.

#### Effective Practices

- ▶ **Legal and Compliance Engagement** – Collaborating with legal and compliance departments to confirm that all agreements supporting control locations are finalized and executed before the accounts are established and coded as good control accounts on firms' books and records.

- ▶ **Addressing Conflicts of Interest** – Confirming which staff have system access to establish a new good control location and that they are independent from the business areas to avoid potential conflicts of interest; and conducting ongoing review to address emerging conflicts of interest.
- ▶ **Reviews and Exception Reports for Good Control Locations** – Conducting periodic review of and implementing exception reports for existing control locations for potential miscoding, out-of-date paperwork or inactivity.
- ▶ **Check-Forwarding Procedures** – Creating and implementing policies to address receipt of customer checks, checks written to the firm, and checks written to a third party.
- ▶ **Check Forwarding Blotter Review** – Creating and reviewing firms’ check received and forwarded blotters to confirm that they are up to date, and including the information required to demonstrate compliance with the Customer Protection Rule exemption.

## Additional Resources

- ▶ [Customer Protection – Reserves and Custody of Securities \(SEA Rule 15c3-3\)](#)
- ▶ U.S. Securities and Exchange Commission, [Custody of Digital Assets Securities by Special Purpose Broker-Dealers](#), Exchange Act Release No. 90,788 (Dec. 23, 2020)
- ▶ U.S. Securities and Exchange Commission, [No-Action Letter to FINRA re: ATS Role in the Settlement of Digital Asset Security Trades](#) (Sept. 25, 2020)

## Appendix—Using FINRA Reports in Your Firm's Compliance Program

Firms have shared the following ways they have used prior FINRA publications, such as Exam Findings Reports and Priorities Letters (collectively, Reports), to enhance their compliance programs. We encourage firms to consider these practices, if relevant to their business model, and continue to provide feedback on how they use FINRA publications.

- ▶ **Assessment of Applicability** – Performed a comprehensive review of the findings, observations and effective practices, and identified those that are relevant to their businesses.
- ▶ **Risk Assessment** – Incorporated the topics highlighted in our Reports into their overall risk assessment process and paid special attention to those topics as they performed their compliance program review.
- ▶ **Gap Analysis** – Conducted a gap analysis to evaluate how their compliance programs and WSPs address the questions noted in Priorities Letters and the effective practices in Exam Findings Reports, and determined whether their compliance programs have any gaps that could lead to the types of findings noted in Exam Findings Reports.
- ▶ **Project Team** – Created interdisciplinary project teams and workstreams (with staff from operations, compliance, supervision, risk, business and legal departments, among other departments) to:
  - assign compliance stakeholders and project owners;
  - summarize current policies and control structures for each topic;
  - engage the legal department for additional guidance regarding regulatory obligations;
  - develop plans to address gaps; and
  - implement effective practices that were not already part of their compliance program.
- ▶ **Circulation to Compliance Groups** – Shared copies of the publications or summaries of relevant sections with their compliance departments.
- ▶ **Presentation to Business Leaders** – Presented to business leadership about their action plans to address questions, findings, observations and effective practices from our Reports.
- ▶ **Guidance** – Used Reports to prepare newsletters, internal knowledge-sharing sites or other notices for their staff.
- ▶ **Training** – Added questions, findings, observations and effective practices from Reports, as well as additional guidance from firms' policies and procedures, to their Firm Element and other firm training.

[www.finra.org](http://www.finra.org)

© 2021 FINRA. All rights reserved.

FINRA and other trademarks of the Financial Industry Regulatory Authority, Inc. may not be used without permission.

21\_0021.1—02/21

# Information Notice

## Imposter Websites Impacting Member Firms

### Summary

Several member firms have recently notified FINRA that they have been victims of imposter websites—which are sites designed to mimic a firm’s actual website with the end goal of committing financial fraud. This *Notice* outlines steps firms can take to monitor for imposter websites and what to do if an imposter website is found.

Questions concerning this *Notice* should be directed to:

- ▶ David Kelley, Surveillance Director, at (816) 802-4729 or [David.Kelley@finra.org](mailto:David.Kelley@finra.org).

### Background and Discussion

Recently, several member firms have informed FINRA that they have experienced challenges related to imposter websites developed by various malicious parties. An imposter website typically is designed to mimic a member firm’s actual website to obtain existing or potential clients’ personally identifiable information (PII) or login credentials, which the website sponsors subsequently use to engage in financial fraud. Malicious parties have been targeting member firms regardless of whether those firms have an existing online presence. In some cases, they have also created email domains and accounts to correspond to the imposter websites. While this is not a new attack strategy, FINRA has observed that the frequency of such attacks on broker-dealers may be increasing.

Member firms can take proactive steps to monitor for imposter websites. For example, firms may consider registering website URL name variations, such as common misspellings or visually similar character substitutions, and using social media or website monitoring services to watch for imposter websites.

April 29, 2019

### Suggested Routing

- ▶ Compliance
- ▶ Information Technology
- ▶ Legal
- ▶ Operations
- ▶ Registered Representatives
- ▶ Risk
- ▶ Senior Management

### Key Topics

- ▶ Cybersecurity
- ▶ Fraud
- ▶ Imposter Websites

If a member firm becomes aware of an imposter website (through its own monitoring, the services of a vendor, notification from a customer or other source), the firm may consider the following actions to address the issue and deactivate the website:

- ▶ Report the attack to local law enforcement, the nearest Federal Bureau of Investigation (FBI) [field office](#) or the Bureau's [Internet Crime Complaint Center](#), and the relevant state's Attorney General via their websites or, if possible, a phone call.<sup>1</sup>
- ▶ Run a "WHOis" search ([www.whois.net](http://www.whois.net)) on the site to determine the hosting provider and domain name registrar associated with the imposter website (which may be the same organization in some instances). In some cases, this site also provides relevant contact information.
- ▶ Submit an abuse report to the hosting provider or the domain registrar asking them to take down the imposter website. Keep the pressure on these providers with repeated calls or emails, or, if necessary, seek the assistance of an attorney, cybersecurity specialist or consultant.
- ▶ Seek the assistance of a cybersecurity specialist attorney or consultant who deals with this type of fraud as they may have some law enforcement or hosting provider contacts or potential legal or other steps not outlined above.
- ▶ Notify the U.S. Securities and Exchange Commission (SEC), FINRA or other securities or financial regulators.
- ▶ Consider posting an alert on your website and sending email notifications to warn clients of the imposter website(s) and the associated URL(s).

If you are a member of Financial Services-Information Sharing and Analysis Center (FS-ISAC) or other information security or cybersecurity controls organizations, please contact them to share information about your attack so they may be able to provide additional mitigation advice.

## Endnote

1. Member firms should consider proactively reaching out to these authorities to establish a relationship. A pre-established relationship can help facilitate the reporting and resolution process when a member firm experiences an attack.

### INFORMATIONAL

## Anti-Money Laundering

### NASD Provides Guidance To Member Firms Concerning Anti-Money Laundering Compliance Programs Required By Federal Law

### SUGGESTED ROUTING

*The Suggested Routing function is meant to aid the reader of this document. Each NASD member firm should consider the appropriate distribution in the context of its own organizational structure.*

- Legal & Compliance
- Operations
- Registration
- Senior Management

### KEY TOPICS

- Compliance Programs
- Money Laundering

### Executive Summary

On October 26, 2001, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act).<sup>1</sup> Title III of the PATRIOT Act, referred to as the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 (Money Laundering Abatement Act), imposes obligations on broker/dealers under new anti-money laundering (AML) provisions and amendments to the existing Bank Secrecy Act (BSA) requirements.<sup>2</sup>

Among other things, the Money Laundering Abatement Act requires all financial institutions, including broker/dealers, to establish and implement, by **April 24, 2002**, AML programs designed to achieve compliance with the BSA and the regulations promulgated thereunder. The NASD reminds members that violations of the AML laws could lead to criminal prosecution.

On February 15, 2002, the NASD filed with the Securities and Exchange Commission (SEC) a rule proposal to prescribe the minimum standards required for each member firm's AML compliance program. A copy of this rule filing can be found on the NASD Regulation AML Web Page. (See [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).) NASD Regulation's AML Web Page also provides links to other sites and documents to assist members in understanding their obligations under the AML rules and regulations.

On February 25, 2002, the SEC published the proposed rule change in the *Federal Register*. The SEC received four comment letters in response to the *Federal Register* publication. Before

becoming effective, the proposed rule change must be approved by the SEC.

The Securities Industry Association Anti-Money Laundering Committee recently released a preliminary guide for firms to use when developing their AML programs (SIA Guidance). The SIA Guidance generally discusses key elements for broker/dealers to consider in developing effective AML programs. NASD Regulation's AML Web Page provides a link to the SIA Guidance.

The NASD is issuing this *Notice* to provide guidance to assist members in developing AML compliance programs that fit their business models and needs. A table of contents has been provided for readers' convenience.

Because the Department of Treasury (Treasury) is still developing AML rules, the NASD will update its guidance as new rules become final. In the interim, firms must comply with the current requirements of the BSA and the provisions of the Money Laundering Abatement Act that now apply to broker/dealers and should familiarize themselves with the proposed rules that Treasury has issued to date. (For links to Treasury's proposed rules, see [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).)

### Questions/Further Information

Questions regarding this *Notice to Members* may be directed to Nancy Libin, Assistant General Counsel, Office of General Counsel, NASD Regulation, at (202) 728-8835; Grace Yeh, Assistant General Counsel, at (202) 728-6939; or Kyra Armstrong, Senior Attorney, Department of Member Regulation, at (202) 728-6962.

## **Anti-Money Laundering Notice to Members**

### **TABLE OF CONTENTS**

<b>BACKGROUND</b>	1
<b>INTRODUCTION</b>	1
<b>Broker/Dealers And Existing Anti-Money Laundering Laws</b>	1
<b>New And Expanded Anti-Money Laundering Laws Applicable To Broker/Dealers</b>	2
<b>NASD ANTI-MONEY LAUNDERING PROGRAM RULE</b>	4
<b>ANTI-MONEY LAUNDERING PROGRAM GUIDANCE</b>	5
<b>Develop Internal Policies, Procedures, And Controls</b>	5
<i><b>Identification And Verification Of Account Holders</b></i>	5
Opening Accounts	5
Online Brokers	7
Additional Due Diligence When Opening an Account	7
<i><b>Prohibitions On U.S. Correspondent Accounts With Foreign Shell Banks And Special Due Diligence For Correspondent Accounts</b></i>	8
<i><b>Special Due Diligence For Private Banking Accounts</b></i>	8
<i><b>Monitoring Accounts For Suspicious Activity</b></i>	9
Money Laundering "Red Flags"	10
Reporting Procedures	11
Recordkeeping And Disclosure	12
Currency Transaction Reports	12
Currency And Monetary Instrument Transportation Reports	12
<i><b>Procedures For Sharing Information With And Responding To Requests For Information From Federal Law Enforcement Agencies</b></i>	12
<i><b>Voluntary Information Sharing Among Financial Institutions</b></i>	13
<b>Designate Compliance Officer</b>	13
<b>Establish An Ongoing Training Program</b>	14
<b>Establish An Independent Testing Function</b>	15
<b>INTRODUCING BROKERS AND CLEARING BROKERS</b>	15
<b>CONCLUSION</b>	16
<b>ENDNOTES</b>	17



## **BACKGROUND**

The PATRIOT Act is designed to detect, deter, and punish terrorists in the United States and abroad and to enhance law enforcement investigation tools by prescribing, among other things, new surveillance procedures, new immigration laws, as well as new and more stringent AML laws. The Money Laundering Abatement Act expands and strengthens the AML provisions put into place by earlier legislation.

Several provisions of the Money Laundering Abatement Act are relevant to NASD members. Among other things, all broker/dealers must implement an anti-money laundering compliance program by April 24, 2002. The Money Laundering Abatement Act also requires Treasury to promulgate rules requiring broker/dealers to file suspicious activity reports (SARs), which identify and describe transactions that raise suspicions of illegal activity, and to establish certain procedures with regard to "correspondent accounts" maintained for foreign banks.<sup>3</sup> In late December 2001, Treasury released proposed rules regarding the filing of SARs by broker/dealers<sup>4</sup> and the maintenance of "correspondent accounts" for foreign banks.<sup>5</sup> In late February 2002, Treasury released proposed and final rules governing information sharing among law enforcement authorities, regulatory organizations, and financial institutions.<sup>6</sup> Treasury will continue to issue proposed and final rules throughout the year governing and providing further guidance with respect to customer identification, "correspondent accounts" with foreign banks, and the application of AML rules to the brokerage industry, among other matters. The NASD will continue to keep members apprised of AML rules and regulations that Treasury proposes and those that Treasury adopts.

## **INTRODUCTION**

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering occurs in connection with a wide variety of crimes, including, but not limited to, drug trafficking, robbery, fraud, racketeering, and terrorism.

In general, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash profits from criminal activity are converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to separate further the proceeds from their criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund further criminal or legitimate activities.<sup>7</sup>

## **Broker/Dealers And Existing Anti-Money Laundering Laws**

Broker/dealers are subject to most of the existing AML rules as well as the new AML provisions of the Money Laundering Abatement Act, which are discussed in detail later in the document.

Firms should be aware that there are potential severe civil and criminal penalties for violations of AML laws. Under the criminal statutes, a person or entity could be criminally prosecuted for assisting or facilitating a transaction involving money laundering by a customer if the firm (or person) knew or was willfully blind to the fact that the transaction involved illegally obtained funds.<sup>8</sup>

---

## Special NASD Notice to Members 02-21

---

All broker/dealers have been and will continue to be subject to existing BSA reporting and recordkeeping requirements, as briefly summarized below:

- **Currency Transaction Report (CTR):** Broker/dealers are required to file CTRs for transactions involving currency that exceed \$10,000. Because structuring is prohibited, multiple transactions are treated as a single transaction if they total more than \$10,000 during any one business day. CTRs are filed with the Financial Crimes Enforcement Network (FinCEN), a bureau of Treasury.
- **Currency and Monetary Instrument Transportation Report (CMIR):** Any person who physically transports, mails, or ships currency or other monetary instruments into or out of the United States, in aggregated amounts exceeding \$10,000 at one time, must report the event on a CMIR. Any person who receives any transport, mail, or shipment of currency, or other monetary instrument from outside the United States in an aggregate amount exceeding \$10,000 at one time also must report the receipt. CMIRs are filed with the Commissioner of Customs.
- **Report of Foreign Bank and Financial Accounts (FBAR):** Any person having a financial interest in, or signature or other authority over, financial accounts in a foreign country is required to report the relationship if the aggregate value of the accounts exceeds \$10,000. FBARs are filed with FinCEN.
- **Funds Transfers and Transmittals:** Broker/dealers effecting transmittals or transfers of funds, including wire fund transfers, of \$3,000 or more must collect, retain and record on the transmittal order certain information regarding the transfer, including the name and address of the transmitter and recipient, the amount of the transmittal order, the identity of the recipient's financial institution, and the account number of the recipient. Broker/dealers also must verify the identity of transmitters and recipients that are not established customers.

In addition, broker/dealers that are subsidiaries of banks or bank holding companies currently are required under the banking regulations to file SARs with FinCEN. Such broker/dealers currently are required to report known or suspected federal criminal offenses, at specified dollar thresholds, or suspicious transactions involving \$5,000 or more that they suspect (1) involve funds derived from illegal activity or an attempt to hide or disguise funds or assets derived from illegal activity, (2) are designed to evade the requirements of the BSA, or (3) have no apparent lawful or business purpose or vary substantially from normal practice. The NASD previously has recommended that members report suspicious transactions and has advised firms that the failure to do so could be construed as aiding and abetting money laundering violations, subjecting the member to civil and criminal liability.<sup>9</sup> Some firms, in fact, have been submitting SARs on a voluntary basis. As discussed in more detail later in the document, all broker/dealers will soon be required to file SARs.

### New And Expanded Anti-Money Laundering Laws Applicable To Broker/Dealers

As noted above, the Money Laundering Abatement Act imposes significant new obligations on broker/dealers through new AML provisions and amendments to the existing provisions of the BSA. A brief summary of the new requirements along with anticipated effective dates is provided below:

- **Section 312 (Due Diligence Requirements):** Section 312 requires special due diligence for all private banking and "correspondent" bank accounts (accounts established to receive deposits from, make payments on behalf of, or handle other financial transactions for a foreign bank) involving foreign persons, even if opened before Congress passed the PATRIOT Act.<sup>10</sup> Treasury is required to delineate, by regulation, the special due diligence

policies, procedures, and controls by April 24, 2002. Regardless of whether final regulations have been promulgated, the minimum due diligence requirements set forth in Section 312 (as discussed below in the “Anti-Money Laundering Program Guidance” section) become **effective on July 23, 2002**.

- **Section 313 (Correspondent Account Prohibitions):** Section 313 prohibits certain financial institutions, including broker/dealers, from maintaining a “correspondent account” for, or on behalf of, a foreign “shell” bank (a foreign bank with no physical presence in any country). Financial institutions are also required to take reasonable steps to ensure that they are not indirectly providing correspondent banking services to foreign shell banks through foreign banks with which they maintain correspondent relationships. Section 313 became **effective on December 26, 2001**. Treasury released proposed regulations defining “correspondent account” in late December 2001.<sup>11</sup>
- **Section 314 (Financial Institution Cooperation Provisions):** Section 314 addresses increased cooperation among financial institutions, regulatory authorities, and law enforcement authorities. Treasury published regulations implementing Section 314 in the *Federal Register* on March 4, 2002.<sup>12</sup> Treasury included a proposed rule to establish a communication link between federal law enforcement and financial institutions to better share information relating to suspected terrorists and money launderers. In addition, Treasury issued an interim final rule, **effective March 4, 2002**, requiring financial institutions to file an initial, and annual thereafter, certification (which can be completed online at FinCEN’s Web Site at [www.treas.gov/fincen](http://www.treas.gov/fincen)) if they wish to share information regarding terrorist financing and money laundering with other financial institutions or associations of financial institutions.<sup>13</sup>
- **Section 319(b) (Domestic and Foreign Bank Records Production):** Section 319(b) addresses the production of domestic and foreign bank records. A financial institution is required to produce account information relating to foreign bank accounts **within seven days** in response to requests from federal law enforcement. Section 319 became **effective on December 26, 2001**. As mentioned above, Treasury released proposed rules regarding maintaining “correspondent accounts” in late December 2001.<sup>14</sup>
- **Section 326 (Customer Identification Standards):** Section 326 requires Treasury and the SEC, jointly, to issue regulations that set forth minimum standards for customer identification in the account opening process. The regulations will need to require firms, at a minimum, to implement “reasonable procedures” to verify the identity of the customer opening an account, maintain records used to identify the customer, and consult government-provided lists of known or suspected terrorists. Final regulations prescribed under Section 326 will take effect **not later than October 26, 2002**. Treasury and the SEC have not yet released proposed regulations regarding customer identification.
- **Section 352 (AML Compliance Program Components):** Section 352 requires all financial institutions to develop and implement AML compliance programs **on or before April 24, 2002**. Section 352 requires the compliance programs, at a minimum, to establish (1) the development of internal policies, procedures, and controls, (2) the designation of a compliance officer with responsibility for a firm’s anti-money laundering program, (3) an ongoing employee training program, and (4) an independent audit function to test the effectiveness of the anti-money laundering compliance program. Section 352 further requires Treasury by April 24, 2002, to issue regulations that consider the extent to which these requirements correspond to the size, location, and activities of different financial institutions. Section 352 further allows Treasury, at its discretion, to issue additional requirements for AML compliance programs before the April 24, 2002, deadline. As further discussed later in the document, the NASD has proposed a rule setting forth the minimum standards for its members’ AML compliance programs.

- **Section 356 (Broker/Dealer SAR Regulations):** By *July 1, 2002*, Treasury must publish final regulations requiring broker/dealers to file SARs. Treasury released proposed broker/dealer SAR regulations in late December 2001.<sup>15</sup> Under Treasury's proposed regulations, the suspicious activity reporting requirement would become effective *180 days after the date on which the final broker/dealer SAR regulations are published in the Federal Register*.

### NASD ANTI-MONEY LAUNDERING PROGRAM RULE

On February 15, 2002, the NASD filed with the SEC a rule proposal that would set forth minimum standards for broker/dealers' AML compliance programs.<sup>16</sup> As required by the Money Laundering Abatement Act itself, the rule proposal would require firms to develop and implement a written AML compliance program by April 24, 2002. The proposed rule would require the program to be approved in writing by a member of senior management and be reasonably designed to achieve and monitor the member's ongoing compliance with the requirements of the BSA and the implementing regulations promulgated thereunder. The proposed rule change would require firms, at a minimum, to:

- (1) establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions;
- (2) establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and implementing regulations;
- (3) provide for independent testing for compliance to be conducted by member personnel or by a qualified outside party;
- (4) designate an individual or individuals responsible for implementing and monitoring the day-to-day operations and internal controls of the program; and
- (5) provide ongoing training for appropriate personnel.

Each firm's AML program must be designed to ensure compliance with the new provisions of the Money Laundering Abatement Act, the earlier provisions of the BSA, and the regulations promulgated thereunder. To be effective, those procedures must reflect the firm's business model and customer base. Further, in developing program criteria, firms should consider the guidelines established by the United States Sentencing Commission in the U.S. Sentencing Commission Guidelines for organizations, as well as the fiduciary responsibilities of officers and directors to ensure that the firm's compliance programs are viable and effective.<sup>17</sup>

Regardless of when and in what form the SEC approves the NASD proposed AML compliance rule, all firms are required by federal law (the Money Laundering Abatement Act) to have AML programs in place **by April 24, 2002**.<sup>18</sup> These AML programs must meet the minimum requirements articulated in Section 352 of the Money Laundering Abatement Act.<sup>19</sup>

Members should keep in mind that the obligation to develop and implement an AML compliance program is not a "one-size-fits-all" requirement. The general nature of the requirement reflects Congressional intent that each financial institution should have the flexibility to tailor its AML program to fit its business. This flexibility is designed to ensure that all entities covered by the statute, from the very large financial institutions to the small firms, will institute effective and appropriate policies and procedures to monitor for AML compliance.<sup>20</sup> In this regard, each broker/dealer, in developing an appropriate AML program that complies with the Money Laundering Abatement Act, should consider factors such as its size, location, business activities, the types of accounts it maintains, and the types of transactions in which its customers engage.

**ANTI-MONEY LAUNDERING PROGRAM GUIDANCE**

The required elements of an AML program are discussed in detail below.

**Develop Internal Policies, Procedures, And Controls**

Broker/dealers must develop internal policies, procedures, and controls to ensure compliance with the AML laws. The AML procedures should contain a statement that sets forth the member's policy of prohibiting money laundering and its overall efforts to detect, deter, and prevent any such violations. Broker/dealers also must establish internal controls to ensure that their AML policies and procedures are being enforced. As with any supervisory procedure, the firm must establish and implement controls and written procedures that explain the procedures that must be followed, the person responsible for carrying out such procedures, how frequently such procedures must be performed, and how compliance with the procedures should be documented and tested.

Firms must determine the manner in which AML procedures that address the following (each of which will be discussed more fully below) will apply to various accounts:

- account opening and maintenance, including verification of the identity of the customer;
- opening and maintaining "correspondent accounts" for foreign banks;
- monitoring of account activities, including but not limited to, trading and the flow of money into and out of the account, the types, amount, and frequency of different financial instruments deposited into and withdrawn from the account, and the origin of such deposits and the destination of withdrawals;
- separating the duties of employees where feasible to ensure a system of checks and balances (for example, firms may want to ensure that persons who handle cash do not open accounts or file CTRs);
- monitoring for, detecting, and responding to "red flags";
- responding to regulatory requests for AML information;
- establishing controls and monitoring employees' trading and financial activity in employee accounts; and
- ensuring that AML compliance programs contain a mechanism or process for the firm's employees to report suspected violations of the firm's AML compliance program procedures and policies to management, confidentially, and without fear of retaliation.

***Identification And Verification Of Account Holders******Opening Accounts***

Prior to the enactment of the Money Laundering Abatement Act, broker/dealers already had significant obligations to gather information about their customers in order to, among other things, know their customers. NASD Rule 3110 requires member firms to obtain certain information about their customers when opening an account, including the following: the customer's name and residence; whether the customer is of legal age; the signature of the registered representative introducing the account and signature of the member or partner, officer, or manager who accepts the account; and if the customer is a corporation, partnership, or other

legal entity, the names of any persons authorized to transact business on behalf of the entity. Member firms are also required to make reasonable efforts to obtain the following additional information (for accounts other than institutional accounts and accounts in which investments are limited to transactions in open-end investment company shares not recommended by the member or its associated persons) prior to the settlement of an initial transaction in the account: a customer's tax identification and Social Security number; the customer's occupation and name and address of the employer; and whether the customer is an associated person of another member.

Member firms also are required under NASD Rules 2110 and 2310 to obtain additional customer information. Members are required under NASD Rule 2110 to comply with general "Know Your Customer" requirements. Pursuant to these requirements, members must make reasonable efforts to obtain certain basic financial information from customers so that members can protect themselves and the integrity of the securities markets from customers who do not have the financial means to pay for transactions.<sup>21</sup> NASD Rule 2310 relates to a member's suitability obligations to its customers and requires each member to use reasonable efforts to obtain information concerning a customer's financial status, tax status, and investment objectives prior to making any recommendations to the customer regarding the purchase, sale, or exchange of securities.

The information required under NASD Rules 3110, 2110, and 2310 is the starting point for new AML customer identification procedures. The Money Laundering Abatement Act imposes additional customer identification requirements on member firms. Effective October 26, 2002 (or earlier, if final customer identification regulations are effective prior to October 26, 2002), broker/dealers are required to implement reasonable procedures for identifying customers and verifying their information.<sup>22</sup> These procedures, at a minimum, must require a firm:

- to verify, to the extent reasonable and practicable, the identity of any customer seeking to open an account;<sup>23</sup>
- to maintain records of information to verify a customer's identity; and
- to check that a customer does not appear on any list of known or suspected terrorists or terrorist organizations such as those persons and organizations listed on Treasury's Office of Foreign Assets Control (OFAC) Web Site ([www.treas.gov/ofac](http://www.treas.gov/ofac)) (and available on [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp)) under "Terrorists" or "Specially Designated Nationals and Blocked Persons" (SDN List), as well as the list of embargoed countries and regions (collectively, the OFAC List).<sup>24</sup>

Under the new AML customer identification requirements, broker/dealers will be required to make reasonable efforts to obtain and verify information about a customer. If the customer is an individual, a firm will need, to the extent reasonable and practicable, to obtain and verify certain information concerning the individual's identity, such as the individual's name, address, date of birth, and government issued identification number. Possible sources of this information include:

- physical documents, such as a driver's license, passport, government identification, or an alien registration card;<sup>25</sup> or, for businesses, a certificate of incorporation, a business license, any partnership agreements, any corporate resolutions, or other similar documents; or
- databases, such as Equifax, Experian, Lexis/Nexis, or other in-house or custom databases.

Firms opening accounts should verify the identification information at the time the account is opened, or within a relatively short time period thereafter (e.g., within five business days after account opening). Because of the unknown risk that the prospective customer could be involved

in criminal activity, members should consider, depending on the nature of a transaction and an account, not effecting a transaction prior to verifying the information. If a potential customer refuses to provide any of the information described above, or appears to have intentionally provided false or misleading information, a firm should not open the account. If an existing customer fails to provide the requested information, the firm, after considering the known and unknown risks involved, may consider closing the account. Moreover, in either of these situations, the firm's AML compliance personnel should be notified so that a determination can be made as to whether the circumstance should be voluntarily reported to FinCEN or OFAC, as appropriate.

In the context of AML compliance, members should implement procedures that allow the firm to collect and use information concerning the account holder's wealth, net worth, and sources of income to detect and deter possible money laundering activity. Such a review should be integrated into the new accounts supervisor's existing procedures before such supervisor authorizes the opening of an account. Moreover, the supervisor's review should be documented and reviewed to ensure that the account-opening procedures are being conducted properly. Firms should consider using a checklist that lists the types of information required and documents explanations for why an account was opened absent such information.

#### *Online Brokers*

Online brokers generally do not meet or speak directly to their prospective or existing clients. These firms must acquire information about customers and, as mentioned earlier, make maximum use of other means of verifying customer identity, such as electronic databases (Equifax, Experion, Lexis/Nexis, or other in-house or custom databases). As is required of all firms, such verification of customer information must take place at the time the account is opened or within a short period thereafter (e.g., five business days). Online firms should also consider conducting computerized surveillance of account activity to detect suspicious transactions and activity. Given the global nature of online brokerage activity, it is essential that online brokers confirm the customer data and review the OFAC List to ensure that customers are not prohibited persons or entities and are not from embargoed countries or regions.

#### *Additional Due Diligence When Opening An Account*

Broker/dealers should perform the following additional due diligence when opening an account, depending on the nature of the account, and to the extent reasonable and practicable:

- inquire about the source of the customer's assets and income so that the firm can determine if the inflow and outflow of money and securities is consistent with the customer's financial status;
- gain an understanding of what the customer's likely trading patterns will be, so that any deviations from the patterns can be detected later on, if they occur;
- maintain records that identify the owners of accounts and their respective citizenship;
- require customers to provide street addresses to open an account, and not simply post office addresses, or "mail drop" addresses;
- periodically contact businesses to verify the accuracy of addresses, the place of business, the telephone, and other identifying information; and
- conduct credit history and criminal background checks through available vendor databases.

***Prohibitions On U.S. Correspondent Accounts With Foreign Shell Banks  
And Special Due Diligence For Correspondent Accounts***

Broker/dealers are prohibited from establishing, maintaining, administering, or managing a “correspondent account” (see note 3) in the United States for an unregulated foreign shell bank. Firms should have procedures in place to ensure that this does not occur and should immediately terminate such accounts if they have any. The broker/dealer’s AML compliance personnel should be notified upon discovery or suspicion that the firm may be maintaining or establishing a “correspondent account” in the United States for a foreign shell bank.

The Money Laundering Abatement Act requires broker/dealers to maintain records identifying the owners of foreign banks that maintain “correspondent accounts” in the United States and the name and address of an agent residing in the United States authorized to accept service of legal process for such banks.<sup>26</sup> Broker/dealers should require their foreign bank account holders to complete model certifications issued by Treasury to the extent possible. U.S. depository institutions and broker/dealers can send the certification forms to their foreign bank account holders for completion. The certification forms generally ask the foreign banks to confirm that they are not shell banks and to provide the necessary ownership and agent information. Use of the certification forms will help firms ensure that they are complying with requirements concerning “correspondent accounts” with foreign banks and can provide a broker/dealer with a safe harbor for purposes of complying with such requirements.<sup>27</sup> Firms are required to recertify (if relying on the certification forms) or otherwise verify any information provided by each foreign bank, or otherwise relied upon, at least every two years or at any time the firm has reason to believe that the information is no longer accurate.

In addition, broker/dealers will be required under Section 312 of the Money Laundering Abatement Act to establish appropriate, specific, and, where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to detect and report instances of money laundering for any “correspondent account” established, maintained, administered, or managed for a foreign bank. *At a minimum*, in the case of foreign banks licensed by certain high-risk jurisdictions or operating under an offshore banking license, broker/dealers are required to take reasonable steps:

- to determine the ownership of the foreign bank;
- to conduct enhanced scrutiny of the account to detect and report suspicious activity; and
- to determine whether the foreign bank maintains “correspondent accounts” for any other bank, and if so, the identity of those banks.<sup>28</sup>

***Special Due Diligence For Private Banking Accounts***

Similarly, the Money Laundering Abatement Act requires broker/dealers, *at a minimum*, to take reasonable steps to determine the identity of the nominal and beneficial account holders of, and the source of funds deposited into, a private banking account maintained by or on behalf of a non-U.S. citizen, and to conduct enhanced scrutiny of accounts requested or maintained by, or on behalf of, a senior foreign political figure,<sup>29</sup> or any immediate family member or close associate of a senior foreign political figure. A private bank account is an account (or combination of accounts) that requires an aggregate deposit of funds or other assets of more than \$1,000,000 established on behalf of one or more individuals who have a direct or beneficial ownership interest in the account, and is assigned to, or administered by, in whole or in part, an officer,



employee, or agent of a financial institution acting as a liaison between the institution and the direct or beneficial owner of the account.<sup>30</sup> This enhanced monitoring or scrutiny should be reasonably designed to detect and report transactions that may involve the proceeds of foreign official corruption.<sup>31</sup> Broker/dealers should monitor future pronouncements from Treasury, while also determining the extent to which they offer “private banking accounts,” and ensure that their AML compliance program includes enhanced monitoring and scrutiny of accounts requested or held on behalf of foreign officials who may be involved in corrupt activities. The special due diligence requirements discussed in this section will become effective on July 23, 2002, regardless of whether Treasury has promulgated final regulations.

### ***Monitoring Accounts For Suspicious Activity***

The Money Laundering Abatement Act requires Treasury to adopt regulations requiring broker/dealers to file SARs.<sup>32</sup> Under Treasury’s proposed regulations, SARs would be filed with FinCEN. Broker/dealers would be required to file SARs for:

- any transaction conducted or attempted by, at or through a broker/dealer involving (separately or in the aggregate) funds or assets of \$5,000 or more for which:
  - the broker/dealer detects any known or suspected federal criminal violation involving the broker/dealer, or
  - the broker/dealer knows, suspects, or has reason to suspect that the transaction:
    - involves funds related to illegal activity,<sup>33</sup>
    - is designed to evade the regulations, or
    - has no business or apparent lawful purpose and the broker/dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Although the reporting threshold begins at \$5,000, in its proposed regulations, Treasury notes that a risk-based approach to developing compliance procedures that can be reasonably expected to promote the detection and reporting of suspicious activity should be the focus of a broker/dealer’s AML compliance program. Treasury further notes that a compliance program that allows for the review of only those transactions that are above a set threshold, regardless of whether transactions at a lower dollar threshold may involve money laundering or other risks, would probably not be a satisfactory program.<sup>34</sup> Broker/dealers should file a SAR and in some circumstances notify law enforcement authorities of all transactions that arouse articulable suspicion that proceeds of criminal, terrorist, or corrupt activities may be involved.

Treasury could amend its proposed regulations based on comments it receives from interested parties. Treasury is required to issue final SAR regulations by July 1, 2002, and firms will be required to file SARs beginning 180 days after final broker/dealer SAR regulations are published in the *Federal Register*. To demonstrate a strong commitment to compliance with AML principles and goals, broker/dealers should consider filing SARs voluntarily prior to the effective date of the regulations. NASD Regulation will keep members informed as Treasury’s proposed regulations are amended and finalized.

*Money Laundering “Red Flags”*

Broker/dealers need to look for signs of suspicious activity that suggest money laundering.<sup>35</sup> If a broker/dealer detects “red flags,” it should perform additional due diligence before proceeding with the transaction. Examples of “red flags” are described below:

- The customer exhibits unusual concern regarding the firm’s compliance with government reporting requirements and the firm’s AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer’s stated business strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm’s policies relating to the deposit of cash and cash equivalents.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force (FATF).<sup>36</sup>
- The customer’s account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer’s account shows numerous currency or cashiers check transactions aggregating to significant sums.
- The customer’s account has a large number of wire transfers to unrelated third parties inconsistent with the customer’s legitimate business purpose.

---

## Special NASD Notice to Members 02-21

---

- The customer's account has wire transfers that have no apparent business purpose to or from a country identified as a money laundering risk or a bank secrecy haven.
- The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)
- The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent business purpose or other purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.<sup>37</sup>

The above-listed money laundering "red flags" are not exhaustive; however, an awareness of the "red flags" will help ensure that broker/dealer personnel can identify circumstances warranting further due diligence. Appropriate "red flags" should be described in the written policies and AML compliance procedures of the broker/dealer.

### *Reporting Procedures*

Although final regulations concerning the filing of SARs may not be adopted until July 1, 2002, voluntary reporting is useful to the government and helpful to firms in order to provide a defense to charges of aiding and abetting money laundering violations. Furthermore, in anticipation of the adoption of the final broker/dealer SAR requirements, all broker/dealers should be preparing to establish and implement procedures to detect and report suspicious transactions by means of SARs. Firms should implement systems, preferably automated ones, that would allow firms to monitor trading, wire transfers, and other account activity to allow firms to determine when suspicious activity is occurring. If a firm decides to monitor customer accounts manually, it must review a sufficient amount of account activity to ensure the detection of suspicious activity by allowing the member to identify patterns of activity and more importantly, new patterns or patterns that are inconsistent with the customer's financial status or make no economic sense.

Exception reports should consider the transaction size, location, type, number, and the nature of the activity. Firms should create guidelines for employees that identify examples of suspicious activity that may involve money laundering and form lists of high-risk clients whose activities may warrant further scrutiny. Firms should develop procedures for following-up on transactions that have been identified as suspicious or high-risk.

Broker/dealers should also develop administrative procedures concerning SARs. The procedures should address the process for filing SARs and reviewing SAR filings and the frequency of filings for continuous suspicious activity. In addition, a broker/dealer should consider requiring that all of its SAR filings be reported periodically to its Board of Directors and/or to senior management. In the event of a high-risk situation, broker/dealers should require that a report be made immediately to the Board of Directors and/or senior management.<sup>38</sup>

#### *Recordkeeping And Disclosure*

Firms should develop procedures to maintain the confidentiality of the SAR filings and to maintain copies of SARs for a five-year period. Firms are prohibited from notifying any person involved in a reported transaction that the transaction has been reported on a SAR. In addition, firms may not disclose SARs or the fact that a SAR was filed, other than to law enforcement agencies or securities regulators. Firms must also have procedures in place to ensure the denial of any subpoena requests for SARs or information in SARs, and for informing FinCEN of any subpoena received. It may be advisable to segregate SAR filings and supporting documentation from other books and records of the firm to avoid violating the prohibitions on disclosure of these records. The broker/dealer should also establish procedures and identify a contact person to handle requests for a subpoena or other requests that call for disclosure of a SAR.

#### *Currency Transaction Reports*

Broker/dealers should have procedures to ensure compliance with the BSA provision requiring broker/dealers to file CTRs with FinCEN.

#### *Currency And Monetary Instrument Transportation Reports*

Broker/dealers should have procedures to ensure compliance with the BSA provision requiring broker/dealers to file CMIRs with the Commissioner of Customs when any person physically transports, receives, mails, or ships currency or other monetary instruments into or out of the United States, in aggregated amounts exceeding \$10,000 at one time.

#### ***Procedures For Sharing Information With And Responding To Requests For Information From Federal Law Enforcement Agencies***

Broker/dealers should develop procedures to handle requests for information from FinCEN relating to money laundering or terrorist activity. Under Treasury's *proposed* regulations implementing Section 314, which were published in the *Federal Register* on March 4, 2002, FinCEN may require broker/dealers to search their records to determine whether they maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. If a broker/dealer identifies an account or transaction identified by FinCEN, it would be required to report the identity of the individual, entity, or organization, the account number, all identifying information provided by the account holder when the account was established, and the date and type of transaction. Broker/dealers would be required to report the information to FinCEN as soon as possible either by e-mail to [patriot@fincen.treas.gov](mailto:patriot@fincen.treas.gov), by calling the Financial Institutions Hotline (1-866-556-3974), or by any other means that FinCEN specifies.

Broker/dealers also should identify contact persons and have procedures in place for providing information to and handling requests from enforcement authorities about the firms' AML efforts, as well as customers engaged in possible money laundering. This information must be provided to the appropriate agency and made available at a specified location when requested. Firms should establish procedures to provide such information *not later than seven days* after receiving a written enforcement agency request.

Firms should also have procedures in place to terminate a correspondent relationship with a foreign bank *within 10 business days* of receiving written notice from Treasury or the United States Attorney General that the foreign bank failed either to comply with a summons or subpoena or to contest it in United States court.

Finally, in the course of performing due diligence or during the opening of an account, firms should immediately contact Federal law enforcement by telephone in appropriate emergency situations as described below:

- a customer is listed on the OFAC List;
- a customer's legal or beneficial account owner is listed on the OFAC List;
- a customer attempts to use bribery, coercion, undue influence, or other inappropriate means to induce a broker/dealer to open an account or proceed with a suspicious or unlawful activity or transaction; and
- any other situation that a firm reasonably determines requires immediate government intervention.

#### ***Voluntary Information Sharing Among Financial Institutions***

To the extent desired and/or appropriate, broker/dealers should have procedures in place for sharing information with other financial institutions about those suspected of terrorism and money laundering. Under Treasury's *interim rule*, which became effective on March 4, 2002, broker/dealers that share this information must file an annual certification with FinCEN.<sup>39</sup> The certification requires broker/dealers to take steps necessary to protect the confidentiality of the information and to use the information only for purposes specified in the rule. The certification can be found at: [www.treas.gov/fincen](http://www.treas.gov/fincen). Broker/dealers should have adequate procedures to protect the security and confidentiality of such information.

#### **Designate Compliance Officer**

Every broker/dealer compliance program must designate a compliance officer ("AML Compliance Officer") to help administer the firm's AML compliance program efforts. Broker/dealers should vest this person with full responsibility and authority to make and enforce the firm's policies and procedures related to money laundering. The AML Compliance Officer does not need to be the firm's current compliance officer. Some larger firms have placed this responsibility on the firm's risk manager. Firms may, however, consider incorporating AML compliance requirements into the existing duties of a firm compliance officer. Whomever the firm designates as its AML Compliance Officer should have the authority, knowledge, and training to carry out the duties and responsibilities of his or her position.

The AML Compliance Officer should monitor compliance with the firm's AML program and help to develop communication and training tools for employees. The AML Compliance Officer should also regularly assist in helping to resolve or address heightened due diligence and "red flag" issues.

The AML Compliance Officer should ensure that AML records are maintained properly and that SARs are filed as required pursuant to the firm's procedures. In short, the AML Compliance Officer should be the primary contact for the firm on AML compliance implementation and oversight.

Finally, to the extent applicable, the AML Compliance Officer should report to a member of the Board of Directors (or other high level executive officer) on AML compliance issues. This senior officer or director should communicate with firm employees on AML issues to further demonstrate the firm's commitment to AML compliance. The firm's senior management should work with the AML Compliance Officer to help ensure that the firm's AML policies, procedures, and programs meet all applicable government standards and that they are effective in detecting, deterring, and punishing or correcting AML misconduct. The firm's senior management also should work with the AML Compliance Officer to ensure that the AML compliance policies, procedures, and programs are updated and reflect current requirements.

### **Establish An Ongoing Training Program**

The Money Laundering Abatement Act requires firms to develop ongoing employee training programs on AML issues. The AML employee training should be developed under the leadership of the AML Compliance Officer or senior management. Educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos are all appropriate training vehicles for AML training. The training may vary based on the type of firm and its size, its customer base, and its resources. The NASD urges its members to instruct their employees about the following topics, at a minimum:

- how to identify "red flags" and possible signs of money laundering that could arise during the course of their duties;
- what to do once the risk is identified;
- what their roles are in the firm's compliance efforts;
- how to perform their roles;
- the firm's record retention policy; and
- disciplinary consequences, including civil and criminal penalties for non-compliance with the Money Laundering Abatement Act.

The NASD advises its members, *at a minimum*, to implement AML training on an annual basis. Frequent evaluation of training programs may be necessary to ensure that firms are informing employees about any new developments with the rules and regulations. As noted above, firms should update their training materials, as necessary, to reflect new developments in the law. Incorporation of money laundering compliance training into continuing education programs is recommended for both registered representatives and supervisors.

A broker/dealer should scrutinize its operations to determine if there are certain employees who may need additional or specialized training due to their duties and responsibilities. For example, employees in Compliance, Margin, and Corporate Security may need more comprehensive training. The firm should train these employees or have these employees receive the appropriate instruction to ensure compliance with the Money Laundering Abatement Act.

**Establish An Independent Testing Function**

In addition to the firm's overall supervisory responsibility to ensure that its procedures are being followed properly, broker/dealers must have an independent testing function to review and assess the adequacy of and level of compliance with the firm's AML compliance program. Either member personnel or a qualified outside party may perform the testing function, depending in part on the firm's size and resources. Smaller firms, for example, may consider using a qualified outside party to complete this function or they may find it more cost effective to use appropriately trained firm personnel. If a firm uses internal personnel, sufficient separation of functions should be maintained to ensure the independence of the internal testing personnel.

The independent testing should be performed annually. After a test is complete, the internal testing personnel or qualified outside party should report its findings to senior management or to an internal audit committee, as appropriate. The firm should ensure that there are procedures for implementation of any of the internal testing personnel's or third party's recommendations and corrective or disciplinary action as the case may warrant.

**INTRODUCING BROKERS AND CLEARING BROKERS**

The NASD wishes to emphasize that both introducing brokers and clearing brokers have responsibilities under the Money Laundering Abatement Act. **All** broker/dealers should devote special attention to potentially high-risk areas for money laundering. Both introducing brokers and clearing brokers must establish and implement the appropriate AML procedures identified above to comply with the Money Laundering Abatement Act's requirements.

In order to detect suspicious activity, it is imperative that introducing and clearing brokers work together to achieve compliance with the Money Laundering Abatement Act. For instance, introducing brokers generally are in the best position to "know the customer," and thus to identify potential money laundering concerns at the account opening stage, including verification of the identity of the customer and deciding whether to open an account for a customer.<sup>40</sup> In essence, introducing brokers should understand that they are the first line of defense in detecting and deterring suspicious activity. Clearing firms, in turn, may be in a better position to monitor customer transaction activity, including but not limited to, trading, wire transfers, and the deposit and withdrawal into and out of accounts of different financial instruments. To assist introducing brokers and, more importantly, satisfy their own obligations under federal law, clearing firms should establish both automated systems to detect suspicious activity and procedures to share AML information and responsibilities with introducing brokers, consistent with the Money Laundering Abatement Act. For example, both the introducing broker and clearing firm may have information concerning a customer relevant to an assessment of whether a wire transfer out of an account to a particular destination raises any AML concerns.

Importantly, introducing brokers must have a basis for assuring themselves that their clearing firms are monitoring customer account activity on their behalf. Similarly, clearing firms must have a basis for assuring themselves that their introducing firms are following appropriate customer identification procedures. Responsibilities relating to AML compliance should be clearly allocated between the parties, and such responsibilities should be specified in the parties' clearing agreements pursuant to NASD Rule 3230. Any such allocation, however, would not relieve either party from its independent obligation to comply with AML laws.

In short, introducing brokers and clearing firms need to work together to allow each firm to meet its obligation to comply with the AML laws.

**CONCLUSION**

As stated above, the NASD will update its guidance as new AML rules and regulations become final. In the interim, the NASD reminds members to comply with the provisions of the Money Laundering Abatement Act that currently apply to broker/dealers. Although the obligation to develop and implement an AML compliance program is not a “one-size-fits-all” requirement, all broker/dealers must have an AML compliance program designed to achieve compliance with the BSA and the regulations promulgated thereunder.



### ENDNOTES

- 1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
- 2 31 U.S.C. §§ 5311, *et seq.*
- 3 In its proposed rules released in December 2001, Treasury defines “correspondent account” for purposes of broker/dealers as “an account established to receive deposits from, make payments on behalf of a foreign bank, or handle other financial transactions related to such bank.” See 66 Fed. Reg. 67,459 (December 28, 2001). The NASD will keep members apprised of any changes to the definition of “correspondent account” when Treasury releases its final rules in this area. Please also note that Treasury’s definition is different from the definition of correspondent brokerage accounts.
- 4 See 66 Fed. Reg. 67,669 (December 31, 2001). NASD Regulation’s AML Web Page provides links to Treasury’s proposed and final regulations.
- 5 See 66 Fed. Reg. 67,459 (December 28, 2001).
- 6 See 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).
- 7 See *generally Anti-Money Laundering, Efforts in the Securities Industry*, Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, GAO-02-111 (October 2001).
- 8 Title 18 U.S.C. §§ 1956 and 1957 make knowingly engaging in, or attempting to engage in, financial transactions involving the proceeds of certain unlawful activities a criminal offense. Therefore, under the criminal statutes, a person or entity could be prosecuted for assisting or participating in money laundering perpetrated by its customer if the firm (or person) knew or was willfully blind to the fact that the transaction involved illegal funds. Criminal penalties include fines up to \$500,000 or twice the value of the property involved in the transaction, whichever is greater, and prison sentences as long as 20 years. In addition to criminal penalties, violators may face civil penalties up to the greater of the value of the property, funds, or monetary interests involved in the transaction or \$10,000, as well as forfeiture of any property involved in the transaction. The BSA also imposes criminal and civil penalties for violations of the BSA or its implementing regulations. Generally, a person can be subject to a criminal fine of up to \$250,000 or imprisonment of up to 5 years, or both. A person who violates the BSA while violating another law of the United States, or engaging in a pattern of illegal activity, is subject to a criminal fine of up to \$500,000 or imprisonment of up to 10 years, or both. The Money Laundering Abatement Act adds additional criminal and civil penalties that can be up to two times the amount of the transaction, not to exceed \$1,000,000 for violations of certain BSA provisions.
- 9 See *NASD Notice to Members 89-12, Reporting Suspicious Currency and Other Questionable Transactions to the IRS/Customs Hotline*.
- 10 See note 3.
- 11 See 66 Fed. Reg. 67,459 (December 28, 2001).
- 12 See 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).
- 13 See 67 Fed. Reg. 9873 (March 4, 2002); 67 Fed. Reg. 9879 (March 4, 2002).
- 14 See 66 Fed. Reg. 67,459 (December 28, 2001).
- 15 See 66 Fed. Reg. 67,669 (December 31, 2001).
- 16 See File No. SR-NASD-2002-24.
- 17 The U.S. Sentencing Commission Guidelines for organizations set out the following criteria for an effective corporate compliance program: (1) whether the company’s compliance standards and procedures are reasonably capable of reducing the prospect of criminal activity; (2) whether there is oversight of the compliance program by high-level personnel; (3) whether the company exercises due care in delegating substantial authority; (4) whether the company communicates effectively to all levels of employees; (5) whether the company has in place viable systems for monitoring, auditing, and reporting suspected misconduct without fear of reprisal; (6) whether the company enforces compliance standards in a consistent manner using appropriate disciplinary measures; and (7) whether the company has taken reasonable steps to respond to and prevent further similar offenses upon detection of a violation. See also *In Re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996); *McCall V. Scott*, 250 F. 3d 1997 (9th Cir. 2001).
- 18 The New York Stock Exchange (NYSE) has also proposed Rule 445, which mirrors the NASD’s proposed rule. See File No. SR-NYSE-2002-10 (filed with the SEC on February 27, 2002).
- 19 31 U.S.C. § 5318(h) (amended by Section 352 of the Money Laundering Abatement Act).
- 20 See *USA Patriot Act of 2001: Consideration of H.R. 3162 Before the Senate* (October 25, 2001) (statement of Sen. Sarbanes); *Financial Anti-Terrorism Act of 2001: Consideration Under Suspension of Rules of H.R. 3004 Before the House of Representatives* (October 17, 2001) (statement of Rep. Kelly) (provisions of the Financial Anti-Terrorism Act of 2001 were incorporated as Title III in the PATRIOT Act.)
- 21 See *Notice to Members 96-32; Notice to Members 96-70; and Notice to Members 99-11*.

## Special NASD Notice to Members 02-21

- 22 Treasury has until October 26, 2002 to promulgate additional customer identification requirements.
- 23 Firms should authenticate customer identity at the time of account opening, and not just when an account shows suspicious activity.
- 24 See *Notice to Members 01-67, Terrorist Activity*. Executive Order 13224 prohibits transactions with those persons and organizations listed on the OFAC Web Site on the SDN List as well as with the listed embargoed countries and regions; See also Section 326 of the Money Laundering Abatement Act. The OFAC Web Site is updated frequently, so members should consult the list on a regular basis. Software programs that allow firms to perform this function in a more user friendly and automated manner are available.
- 25 Note that under the BSA, firms must record a current passport number or other valid government identification number for transfers or transmittals of \$3,000 or more by or for non-resident alien accounts. See 31 C.F.R. 103.33 (2001).
- 26 31 U.S.C. § 5318(k) (amended by Section 319(b) of the Money Laundering Abatement Act).
- 27 31 U.S.C. § 5318(j) (amended by Section 313 of the Money Laundering Abatement Act). Please note that Treasury included a model certification form in its December 2001 rule proposal, available at [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).
- 28 31 U.S.C. § 5318(i) (amended by Section 312 of the Money Laundering Abatement Act).
- 29 Treas. Dept., Bd. of Gov. of Fed. Res., Comp. Of the Currency, F.D.I.C., O.T.S. and State Dept., *Guidance on Enhanced Scrutiny for Transactions that May Involve the Proceeds of Foreign Official Corruption*, (Jan. 2001) and at [www.ustreas.gov/press/releases/guidance.htm](http://www.ustreas.gov/press/releases/guidance.htm).
- 30 31 U.S.C. § 5318(i) (amended by Section 312(a)(i)(4)(B) of the Money Laundering Abatement Act).
- 31 31 U.S.C. § 5318(i) (amended by Section 312(a)(i)(3) of the Money Laundering Abatement Act).
- 32 31 U.S.C. § 5318(g).
- 33 Evidence that a broker/dealer knows that the property involved in a financial transaction constitutes the proceeds of unlawful activity and nonetheless conducts (or attempts to conduct) the financial transaction with the unlawful proceeds with the intent to promote the unlawful activity or knowing that the transaction is designed to conceal or disguise the nature, source, or ownership of the unlawful proceeds, can subject a broker/dealer to criminal prosecution. See 18 U.S.C. § 1956.
- 34 66 Fed. Reg. 67,669 at 67,674 (Dec. 31, 2001).
- 35 Firms are also reminded to notify self-regulatory organizations and the SEC if they detect indicators of securities laws violations. Firms should note that there are exceptions to the proposed broker/dealer SAR requirements, including that a broker/dealer is not required to file a SAR to report a possible violation of any of the federal securities laws or rules of a self-regulatory organization by the broker/dealer or any of its officers or directors, employees, or other registered representatives, other than certain rules, so long as such violation is properly reported to the SEC or a self-regulatory organization. See 66 Fed. Reg. 67,669 at 67,676-677 (Dec. 31, 2001).
- 36 The FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering. The FATF monitors members' progress in implementing anti-money laundering measures, reviews money laundering techniques and counter-measures, and promotes the adoption and implementation of anti-money laundering measures globally. See links to the FATF Web Site at [www.nasdr.com/money.asp](http://www.nasdr.com/money.asp).
- 37 See Speech by Lori Richards, Director of Securities and Exchange Commission's Office of Compliance Inspections and Examinations, *Money Laundering: It's on the SEC's Radar Screen* (May 8, 2001); See also SIA, *Preliminary Guidance for Deterring Money Laundering Activity*, at 12-13 (Feb. 2002); Sarah B. Estes, Sutherland, Asbill & Brennan LLP, *Securities Broker-Dealers and Money Laundering: The Obligations of Broker-Dealers Under Money Laundering Laws* at 5-6 (2001).
- 38 Firms may wish to consult FinCEN's Web Site for more information (see [www.treas.gov/fincen](http://www.treas.gov/fincen)), including, annual SAR Activity Review reports and SAR Bulletins, which discuss trends in suspicious activity reporting and give helpful tips.
- 39 See 67 Fed. Reg. 9873 (March 4, 2002).
- 40 All broker/dealers should consider using electronic databases (such as Equifax, Experion, Lexis/Nexis, or other in-house or custom databases) to verify customer identity.

© 2002 National Association of Securities Dealers, Inc. (NASD). All rights reserved. Notices to Members attempt to present information to readers in a format that is easily understandable. However, please be aware that, in case of any misunderstanding, the rule language prevails.

## Customer Assets

### Verification of Instructions to Transmit or Withdraw Assets from Customer Accounts

#### Executive Summary

As part of their duty to safeguard customer assets and to meet their supervisory obligations, FINRA firms must have and enforce policies and procedures governing the withdrawal or transmittal of funds or other assets from customer accounts.<sup>1</sup> Among other things, the policies and procedures should be reasonably designed to review and monitor all instructions to transmit or withdraw assets from customer accounts, including instructions from an investment adviser or other third party purporting to act on behalf of the customer. FINRA firms are required to test and verify their procedures for adequacy and to update them when necessary.

Questions concerning this *Notice* should be addressed to:

- Mike Rufino, Senior Vice President and Deputy, Member Regulation, at (212) 858-4487; or
- Patricia Albrecht, Assistant General Counsel, Office of General Counsel, at (202) 728-8026.

#### Background and Discussion

Recently, several cases involving the misappropriation of customer assets have highlighted the importance of having adequate procedures for verifying the validity of instructions to transmit or withdraw securities or other assets from customer accounts. In some cases, an employee of the firm committed a fraud; in others, outside investment advisers or other third parties purported to be acting on behalf of the customer. A number of the cases involved forged letters of authorization. In some, employees concealed their misconduct by diverting customers' genuine account statements to a post office box or address under the employee's control, and replacing them with fabricated statements.

November 2009

#### Notice Type

- Guidance

#### Suggested Routing

- Compliance
- Legal
- Operations
- Senior Management

#### Key Topic(s)

- Internal Controls
- Letters of Authorization
- Supervisory Procedures
- Transmittal/Withdrawal of Customer Assets

#### Referenced Rules & Notices

- Information Notice 3/12/08
- NASD Rule 3012
- NYSE Rule 342.23
- NYSE Rule 401



### Policies and Procedures

NASD Rule 3012 (Supervisory Control System)<sup>2</sup> and Incorporated NYSE Rule 401 (Business Conduct) require all firms to establish, maintain and enforce written supervisory control policies and procedures that, among other things, include procedures that are reasonably designed to review and monitor the transmittal of funds (*e.g.*, wires or checks) or securities:

- from customer accounts to third-party accounts (*i.e.*, a transmittal that would result in a change of beneficial ownership);
- from customer accounts to outside entities (*e.g.*, banks, investment companies);
- from customer accounts to locations other than a customer's primary residence (*e.g.*, post office box, "in care of" accounts, alternate address); and
- between customers and registered representatives (including the hand-delivery of checks).

The policies and procedures a firm establishes under these rules must include "a means or method of customer confirmation, notification or follow up that can be documented."<sup>3</sup> NASD Rule 3012 further provides that a firm must identify in its written supervisory control procedures any of these activities it does not engage in and document that additional supervisory policies and procedures for such activities must be in place before the firm can engage in them.<sup>4</sup>

These rules apply to both clearing and introducing firms. While firms may allocate responsibility for complying with particular requirements between the clearing and introducing firms, both firms must have policies and procedures in place to ensure that their respective responsibilities are met. For example, the firms may agree that the introducing firm is responsible for verifying a customer's identity. However, the clearing firm must still have adequate policies and procedures to review and monitor disbursements it makes to third-party accounts, outside entities or an address other than the customer's primary address. A firm's procedures should also specify how instructions to withdraw or transmit assets may be conveyed, including which employees of the introducing firm are authorized to transmit instructions to the clearing firm on the customer's behalf, and both firms are responsible for ensuring that their employees follow their respective procedures.

Additionally, a firm's policies and procedures should include procedures that are reasonably designed to, among other things:

- Verify that any third party who purports to be acting on behalf of a customer, including any family member, third-party investment advisor or money manager, has been authorized by the customer to take the action in question. Typically, this requires firms to verify that a valid power of attorney has been executed by the customer and that actions taken by the third party are within the scope of the authority conveyed.
- Verify the identity of a person who appears in person to receive assets and who claims to be the customer.
- Adequately document the steps taken to verify the information listed above and maintain that documentation in accordance with applicable books and records requirements.
- Identify and respond to red flags or suspicious activity.

If a firm's procedures require heightened review of certain transmittal instructions based on dollar amount thresholds, firms should also be aware that firm employees or third-party investment advisers can learn of the threshold amounts and try to "fly under the radar" by submitting multiple instructions for lesser amounts. Therefore, firms should take steps to address this risk, including, to the extent possible, limiting dissemination of information about the threshold triggers.

While firms' procedures must be designed to detect and respond to unusual or suspicious activity, firms must also take into account that fraudulent activity can often flourish when employees fall into a sense of familiarity or routine that can be exploited either by other employees or third parties. Therefore, firms must train their employees to follow all applicable policies and procedures rigorously, even in what appear to be routine situations. Moreover, a firm's policies and procedures should include random sampling and testing of even routine transfers and withdrawals. This helps to verify that employees follow agreed upon procedures and helps deter improper conduct. In addition, firms should closely monitor the use of standing instructions, including standing letters of authorization. Parameters for the instructions should be clear and the authorization kept current.

Firms that use automated systems to help monitor transmittals and withdrawals must have adequate means to test and review the effectiveness of such systems just as they must monitor manual systems. Firms should also periodically review and assess the adequacy of their automated supervisory systems and procedures, which can become outdated or ineffective for a variety of reasons, including business growth, consolidation, new technologies, as well as changes in the size, volume and/or frequency of transmittals. Firms are also reminded to make certain that each employee's access to relevant systems is limited strictly to what is appropriate for the employee's function within the firm.

### Questions to Consider

Given the recent number of cases involving fraudulent letters of authorization and other forms of transmittal requests, FINRA urges firms to review the adequacy of their current policies and procedures to verify the validity of such requests. As they do so, firms may find the following questions helpful:

- What types of transmittals does the firm accept?
- Do the firm's policies and procedures adequately address all types of permitted transmittals, as well as FINRA's requirements that firm's have procedures specifically designed to review and monitor these transmittals?
- How are transmittals identified on the firm's books and records, and what exception reports are used to monitor them? Is there any type of transmittal that is not included in exception reports?
- Does the person(s) responsible for reviewing transmittals have a means to review all transmittals regardless of the form in which they are submitted?
- If standing letters of authorization are permitted, are there limits on their use? Do they expire after a specified period of time? Are transfers made pursuant to standing letters of authorization subject to heightened scrutiny?
- Is there a tracking and/or reconciliation process for transmittals?
- Do the firm's procedures adequately address risks associated with the various ways it allows transmittal requests to be communicated (telephone, fax, email, notarized letter)?
- Are there clear guidelines for employees regarding letters of authorization and have they been communicated effectively? Do these guidelines allow exceptions, and if so, how are they documented?
- Is there a separate system to follow up and review the letter of authorization process, and is the level of testing adequate? Are all types of transmittals, based on dollar amount or format, potentially subject to independent verification and testing?
- Do testing procedures include representative samples of transaction types, volumes and dollar amounts?
- If procedures include thresholds or parameters to identify transmittals subject to heightened supervision or additional testing, are the parameters adequate given the current transaction volume and average dollar size? Can parties circumvent the parameters by using multiple, smaller transfers that are designed to "fly under the radar"?

- Do any non-employees have access and/or authority over part of the transmittal process (such as signature verification at an introducing broker)? What types of tests are used to ensure that access and authority is properly limited?
- Are there adequate and clearly communicated escalation procedures for bringing red flags or suspicious activity to senior management's attention?

For more information, please listen to FINRA's compliance podcast, which highlights strong practices based on a survey of a sample of FINRA firms. The podcast, "Letters of Authorization," was published on January 21, 2009, and is available at [www.finra.org/podcasts](http://www.finra.org/podcasts).

## Endnotes

- 1 This *Notice* does not apply to account transfers made pursuant to ACATS or FINRA Rule 11870.
- 2 The current FINRA rulebook consists of (1) FINRA Rules; (2) NASD Rules; and (3) rules incorporated from NYSE (Incorporated NYSE Rules) (together, the NASD Rules and Incorporated NYSE Rules are referred to as the Transitional Rulebook). While the NASD Rules generally apply to all FINRA member firms, the Incorporated NYSE Rules apply only to those member firms of FINRA that are also members of the NYSE (Dual Members). The FINRA Rules apply to all FINRA member firms, unless such rules have a more limited application by their terms. For more information about the rulebook consolidation process, see *Information Notice 3/12/08* (Rulebook Consolidation Process).
- 3 See NASD Rule 3012(a)(2)(B) and Incorporated NYSE Rule 401(b) (requiring procedures as part of a firm's internal control requirements prescribed under Incorporated NYSE Rule 342.23).
- 4 See NASD Rule 3012(a)(2)(B). Incorporated NYSE Rule 401 does not have a comparable provision.

© 2009 FINRA. All rights reserved. FINRA and other trademarks of the Financial Industry Regulatory Authority, Inc. may not be used without permission. *Regulatory Notices* attempt to present information to readers in a format that is easily understandable. However, please be aware that, in case of any misunderstanding, the rule language prevails.

## Customer Account Protection

### Verification of Emailed Instructions to Transmit or Withdraw Assets From Customer Accounts

#### Executive Summary

FINRA has received an increasing number of reports of incidents of customer funds stolen as a result of instructions emailed to firms from customer email accounts that have been compromised. These incidents highlight some of the risks associated with accepting instructions to transmit or withdraw funds via email. FINRA recommends that firms reassess their policies and procedures to ensure they are adequate to protect customer assets from such risks. The Federal Bureau of Investigation (FBI), Financial Services Information Sharing and Analysis Center (FS-ISAC) and Internet Crime Complaint Center (IC3) recently released a joint fraud alert describing a similar trend.<sup>1</sup>

Questions concerning this *Notice* should be addressed to:

- ▶ Patricia Albrecht, Associate General Counsel, Office of General Counsel, at (202) 728-8026; or
- ▶ Terry H. Miller, Lead Sr. Regulatory Specialist, Member Regulation Department, at (202) 728-8159.

#### Background and Discussion

FINRA has received an increasing number of reports of incidents in which firms have wired customer funds to third-party accounts based on instructions received from customers' email accounts that had been compromised by third parties. In some instances, the perpetrators appear to have obtained customers' brokerage information by accessing customers' email accounts and searching contact lists or emails sent from the account. Typically, the perpetrators of these fraudulent schemes email brokerage firms from customers' personal email accounts with instructions to wire funds to an account, often overseas, controlled by the perpetrator. The instructions may be accompanied or followed by fraudulent letters of authorization also emailed from compromised email accounts. In some instances, firms have released funds after unsuccessfully attempting to verify emailed instructions by phone. In at least one case, the fraudulent email stressed the urgency of the requested transfer, pressuring the firm to release the funds before verifying the authenticity of the emailed instructions.

January 2012

#### Notice Type

- ▶ Special Alert

#### Suggested Routing

- ▶ Operations
- ▶ Senior Management
- ▶ Systems

#### Key Topics

- ▶ Customer Account Protection

#### Referenced Rules & Notices

- ▶ FINRA Rule 4311
- ▶ FTC FACT Act
- ▶ NASD Rule 3012
- ▶ NYSE Rule 401
- ▶ Regulatory Notice 08-69
- ▶ Regulatory Notice 09-64



## Policies and Procedures

NASD Rule 3012 (Supervisory Control System)<sup>2</sup> and Incorporated NYSE Rule 401 (Business Conduct) require all firms to establish, maintain and enforce written supervisory control policies and procedures that, among other things, include procedures that are reasonably designed to review and monitor the transmittal of funds (*e.g.*, wires or checks) or securities:

- ▶ from customer accounts to third-party accounts (*i.e.*, a transmittal that would result in a change of beneficial ownership);
- ▶ from customer accounts to outside entities (*e.g.*, banks, investment companies);
- ▶ from customer accounts to locations other than a customer's primary residence (*e.g.*, post office box, "in care of" accounts, alternate address); and
- ▶ between customers and registered representatives (including the hand-delivery of checks).

The policies and procedures a firm establishes under these rules must include "a means or method of customer confirmation, notification or follow up that can be documented."<sup>3</sup>

NASD Rule 3012 further provides that a firm must identify in its written supervisory control procedures any of these activities in which it does not engage, and document that additional supervisory policies and procedures for such activities must be in place before the firm can engage in them.<sup>4</sup>

FINRA addressed the scope of these obligations in [Regulatory Notice 09-64](#), which highlighted a number of questions firms should consider in assessing the adequacy of their policies and procedures for verifying the validity of requests to withdraw or transfer customer funds. Among other things, FINRA noted that firms should ensure that their procedures adequately address the specific risks associated with each method the firm allows for transmitting instructions.

One of the risks associated with accepting instructions to withdraw or transfer funds by email and other electronic means is that customers' email accounts are susceptible to being breached by hackers or other intruders who may use the email accounts to commit fraud. Therefore, FINRA recommends that firms reassess their policies and procedures for accepting instructions to withdraw or transfer funds via electronic means to ensure that they are adequately designed to protect customer accounts from the risk that customers' email accounts may be compromised and used to send fraudulent transmittal or withdrawal instructions. Among other things, FINRA recommends that such policies and procedures should:

- ▶ include a method for verifying that the email was in fact sent by the customer; and
- ▶ be designed to identify and respond to "red flags," including transfer requests that are out of the ordinary, requests that funds be transferred to an unfamiliar third party account,<sup>5</sup> or requests that indicate urgency or otherwise appear designed to deter verification of the transfer instructions.

As FINRA noted in [Regulatory Notice 09-64](#), firms must train their employees to follow all applicable policies and procedures rigorously. Firms' policies and procedures should also include random sampling and testing of transfers and withdrawals to monitor for compliance.<sup>6</sup>

As noted in [Regulatory Notice 09-64](#), the requirement that firms have supervisory procedures for reviewing and monitoring transfers of customer assets applies to both clearing and introducing firms. Further, FINRA Rule 4311(c) requires that when customer accounts are to be carried on a fully disclosed basis, the carrying agreement must specify the responsibilities of each party to the agreement, and while the rule permits firms to allocate responsibility for the performance of certain functions between the carrying and introducing firms, it expressly requires that the carrying firm be allocated the responsibility for the safeguarding of customer funds and securities. Both firms must have policies and procedures in place to ensure that their respective regulatory and contractual responsibilities are met. For example, the firms may agree that the introducing firm is responsible for verifying a customer's identity and that the instructions originated with the customer, in which case the introducing firm must have adequate policies and procedures to ensure that it effectively carries out this function.

However, the carrying firm must still have adequate policies and procedures to review and monitor all disbursements it makes from customers' accounts, including but not limited to third-party accounts, outside entities or an address other than the customer's primary address. A firm's procedures should also specify how instructions to withdraw or transmit assets may be conveyed, including which employees of the introducing firm are authorized to transmit instructions to the clearing firm on the customer's behalf, and both firms are responsible for ensuring that their employees follow their respective procedures.

Firms should also consider advising customers to notify the firm if a customer discovers that his or her email account has been compromised. Firms receiving such notification should have a method for ensuring that the information is communicated and used effectively within the firm to protect both the customer accounts and the firm.

## Conclusion

Given the rise in incidents reported to FINRA involving fraud perpetrated through compromised customer email accounts, FINRA recommends that firms reassess their specific policies and procedures for accepting and verifying instructions to withdraw or transfer customer funds that are transmitted via email or other electronic means, as well as firms' overall policies and procedures in this area.

1. Fraud Alert Involving E-mail Intrusions to Facilitate Wire Transfers Overseas, January 20, 2012, at <http://www.ic3.gov/media/2012/EmailFraudWireTransferAlert.pdf>.
2. The current FINRA rulebook consists of (1) FINRA Rules; (2) NASD Rules; and (3) rules incorporated from NYSE (Incorporated NYSE Rules). While the NASD Rules generally apply to all FINRA member firms, the Incorporated NYSE Rules apply only to those member firms of FINRA that are also members of the NYSE (Dual Members). The FINRA Rules apply to all FINRA member firms, unless such rules have a more limited application by their terms. For more information about the rulebook consolidation process, see [Information Notice 3/12/08](#) (Rulebook Consolidation Process).
3. See NASD Rule 3012(a)(2)(B) and Incorporated NYSE Rule 401(b) (requiring procedures as part of a firm's internal control requirements prescribed under Incorporated NYSE Rule 342.23).
4. See NASD Rule 3012(a)(2)(B). Incorporated NYSE Rule 401 does not have a comparable provision.
5. In this regard, firms might consider having customers indicate in writing parties to whom they might make transfers as a check against unfamiliar third party transfers.
6. Firms are also reminded that the Federal Trade Commission (FTC) and the federal banking regulators have issued joint regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). Among other things, the FTC's regulations, which apply to most member firms, require that financial institutions develop and implement a written program to detect, prevent and mitigate identity theft in connection with the opening of certain accounts or the maintenance of certain existing accounts (referred to as the Red Flags Rule). See Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 FR 63718 (November 9, 2007) (Joint Final Rules and Guidelines of the FTC, Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), and National Credit Union Administration (NCUA)). See Pub. L. 108-159 (amending Section 615 of the Fair Credit Reporting Act of 1970 (FCRA) and adding new Section 605(h)(2)). For more information on the applicability of the FTC Red Flags Rule to FINRA member firms, see [Regulatory Notice 08-69](#) (November 2008).



Peshkova/iStock/Getty Images Plus

PRACTICE MANAGEMENT &gt; REGULATION &amp; COMPLIANCE

## 'Pig-Butchering' Scams a Top Investor Threat, According to State Regulators

*The oddly named scheme, where a fraudster will bleed the victim's finances in small increments, akin to fattening up a pig before they're slaughtered, is gaining ground in the crypto space.*

Patrick Donachie | Apr 20, 2023

A particular kind of scam is hogging the attention of state securities regulators.

So-called pig-butchering schemes are becoming increasingly prominent in the cryptocurrency space, and 46% of state regulators in the U.S. and Canada say these

type of scams are a top concern, according to the North American Securities Administrators Association's annual list of top investor threats.

Pig-butcher schemes were the second-most-cited threat by U.S. and Canadian state securities regulators responding to NASAA's survey, marking the first time the threat has made the list. Digital asset frauds took the top spot, cited by 62% of respondents, while social media and internet schemes followed behind, at 41%.

The term "pig-butcher" came to greater prominence as crypto hit the mainstream, and these schemes often take the guise of crypto opportunities, according to Amanda Senn, NASAA's Enforcement Committee co-chair and chief deputy director for the Alabama Securities Commission.

Often, the fraudster will contact the victim through social media apps or texting, touting their success with an (often fraudulent) crypto exchange. The fraudster commits them to a small sum of money at first and provides small returns, lending a degree of credibility at a time.

This is where the term's significance comes in, Senn explained; in lieu of trying for a lump sum, the fraudster will bleed the victim's finances in small increments, akin to fattening up a pig before they're slaughtered.

"And then the fraudster goes for the kill," she said. "They take more and more money from the victim before a total loss is experienced by the victim."

Alabama securities regulators have gone after numerous pig-butcher schemes, citing two cases this year with alleged fraudsters purporting to be online cryptocurrency exchanges with no known business addresses. Senn said investors had lost millions in her state alone, and she worried that victims might be vulnerable to crypto-related schemes because they wouldn't know how to find legitimate investments in the space.

Such schemes could also rebound on broker/dealers and advisors working with victims, particularly if money comes out of the victim's brokerage account, according to Sander Ressler, a managing director of Essential Edge Compliance Outsourcing Services.

When a victim learns of the scam, they may ask their broker about why they didn't question its validity. Brokerage firms will often have different supervisory requirements when sending money to a third party.

---

**Source URL:**<https://www.wealthmanagement.com/regulation-compliance/pig-butchering-scams-top-investor-threat-according-state-regulators>

## FinCEN's Customer Due Diligence Requirements for Financial Institutions and FINRA Rule 3310

**FINRA Provides Guidance to Firms Regarding Anti-Money Laundering Program Requirements Under FINRA Rule 3310 Following Adoption of FinCEN's Final Rule to Enhance Customer Due Diligence Requirements for Financial Institutions**

### Summary

FINRA is issuing this *Notice* to provide guidance regarding member firms' obligations under FINRA Rule 3310 (Anti-Money Laundering Compliance Program) in light of the Financial Crimes Enforcement Network's (FinCEN) adoption of a final rule on Customer Due Diligence Requirements for Financial Institutions (CDD Rule).

FinCEN's CDD Rule became effective July 11, 2016. Member firms must be in compliance with its provisions by May 11, 2018.

Questions concerning this *Notice* should be directed to:

- ▶ Michael Rufino, Executive Vice President, Head of Member Regulation — Sales Practice, at (212) 858-4487 or by email at [Michael.Rufino@finra.org](mailto:Michael.Rufino@finra.org);
- ▶ Victoria Crane, Associate General Counsel, Office of General Counsel, at (202) 728-8104 or by email at [Victoria.Crane@finra.org](mailto:Victoria.Crane@finra.org); or
- ▶ Meredith Cordisco, Associate General Counsel, Office of General Counsel, at (202) 728-8018 or by email at [Meredith.Cordisco@finra.org](mailto:Meredith.Cordisco@finra.org).

**November 21, 2017**

### Notice Type

- ▶ Guidance

### Suggested Routing

- ▶ Compliance
- ▶ Legal
- ▶ Operations
- ▶ Senior Management

### Key Topics

- ▶ Anti-Money Laundering
- ▶ Compliance Programs

### Referenced Rules & Notices

- ▶ 31 CFR 1023.210, Bank Secrecy Act
- ▶ FINRA Rule 3310



## Background & Discussion

The Bank Secrecy Act<sup>1</sup> (BSA), among other things, requires financial institutions,<sup>2</sup> including broker-dealers, to develop and implement anti-money laundering (AML) programs that, at a minimum, meet the statutorily enumerated “four pillars.”<sup>3</sup> These four pillars require broker-dealers to have written AML programs that include, at a minimum:

- ▶ the establishment and implementation of policies, procedures and internal controls reasonably designed to achieve compliance with the applicable provisions of the BSA and implementing regulations;
- ▶ independent testing for compliance by broker-dealer personnel or a qualified outside party;
- ▶ designation of an individual or individuals responsible for implementing and monitoring the operations and internal controls of the AML program; and
- ▶ ongoing training for appropriate persons.<sup>4</sup>

In addition to meeting the BSA’s requirements with respect to AML programs, broker-dealers must also comply with FINRA Rule 3310, which incorporates the BSA’s four pillars, including requiring broker-dealers’ AML programs to establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions.

On May 11, 2016, FinCEN, the bureau of the Department of the Treasury responsible for administering the BSA and its implementing regulations, issued the CDD Rule<sup>5</sup> to clarify and strengthen customer due diligence for covered financial institutions,<sup>6</sup> including broker-dealers. In its 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.<sup>7</sup> As the first component is already an AML program requirement, the CDD Rule focuses on the other three components.

Specifically, the CDD Rule focuses particularly on the second component by adding a new requirement that covered financial institutions identify and verify the identity of the beneficial owners of all legal entity customers at the time a new account is opened, subject to certain exclusions and exemptions. The CDD Rule also addresses the third and fourth components, which FinCEN states “are already implicitly required for covered financial institutions to comply with their suspicious activity reporting requirements,” by amending the existing AML program rules for covered financial institutions to explicitly require these components to be included in AML programs as a new “fifth pillar.” As a result of the CDD Rule, member firms should ensure that their AML programs are updated, as necessary, to comply with the CDD Rule by May 11, 2018.



This *Notice* provides guidance to member firms regarding their obligations under FINRA Rule 3310 in light of the adoption of FinCEN's CDD Rule. In addition, the *Notice* summarizes the CDD Rule's impact on member firms, including the addition of the new fifth pillar required for member firms' AML programs. Member firms should also consult the CDD Rule as well as FinCEN's related FAQs,<sup>8</sup> which FinCEN indicates it will periodically update.

### **FINRA Rule 3310 and Amendments to Minimum Requirements for Member Firms' AML Programs**

Section 352 of the USA PATRIOT Act of 2001<sup>9</sup> amended the BSA to require broker-dealers to develop and implement AML programs that include the four pillars mentioned above. Consistent with Section 352 of the PATRIOT Act, and incorporating the four pillars, FINRA Rule 3310 requires each member firm to develop and implement a written AML program reasonably designed to achieve and monitor the member firm's compliance with the BSA and implementing regulations. Among other requirements, FINRA Rule 3310 requires that each member firm, at a minimum: (1) establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions; (2) establish and implement policies, procedures, and internal controls reasonably designed to achieve compliance with the BSA and implementing regulations; (3) provide for annual (on a calendar-year basis) independent testing for compliance to be conducted by member firm personnel or a qualified outside party;<sup>10</sup> (4) designate and identify to FINRA an individual or individuals (*i.e.*, AML compliance person(s)) who will be responsible for implementing and monitoring the day-to-day operations and internal controls of the AML program and provide prompt notification to FINRA of any changes to the designation; and (5) provide ongoing training for appropriate persons.

FinCEN's CDD Rule does not change the requirements of FINRA Rule 3310, and member firms must continue to comply with its requirements.<sup>11</sup> However, FinCEN's CDD Rule 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.<sup>12</sup> This ongoing customer due diligence element, or "fifth pillar" required for AML programs, includes: (1) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (2) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.<sup>13</sup> As stated in the CDD Rule, these provisions are not new and merely codify existing expectations for firms to adequately identify and report suspicious transactions as required under the BSA and encapsulate practices generally undertaken already by securities firms to know and understand their customers.<sup>14</sup> However, to the extent that these elements, which are briefly summarized below, are not already included in member firms' AML programs, the CDD Rule requires member firms to update their AML programs to explicitly incorporate them.

FINRA is considering whether further rulemaking is necessary to more closely align FINRA Rule 3310 with FinCEN's CDD Rule in light of the now-codified fifth pillar requirement for firms' AML programs.

## Summary of Fifth Pillar's Requirements

### Understanding the Nature and Purpose of Customer Relationships

FinCEN states in the CDD Rule that firms must necessarily have an understanding of the nature and purpose of the customer relationship in order to determine whether a transaction is potentially suspicious and, in turn, to fulfill their suspicious activity reporting obligations.<sup>15</sup> To that end, the CDD Rule requires that firms understand the nature and purpose of the customer relationship in order to develop a customer risk profile. The customer risk profile refers to information gathered about a customer to form the baseline against which customer activity is assessed for suspicious transaction reporting.<sup>16</sup> Information relevant to understanding the nature and purpose of the customer relationship may be self-evident and, depending on the facts and circumstances, may include such information as the type of customer, account or service offered, and the customer's income, net worth, domicile, or principal occupation or business, as well as, in the case of existing customers, the customer's history of activity.<sup>17</sup> The CDD Rule also does not prescribe a particular form of the customer risk profile.<sup>18</sup> Instead, the CDD Rule states that depending on the firm and the nature of its business, a customer risk profile may consist of individualized risk scoring, placement of customers into risk categories or another means of assessing customer risk that allows firms to understand the risk posed by the customer and to demonstrate that understanding.<sup>19</sup>

The CDD Rule also addresses the interplay of understanding the nature and purpose of customer relationships with the ongoing monitoring obligation discussed below. The CDD Rule explains that firms are not necessarily required or expected to integrate customer information or the customer risk profile into existing transaction monitoring systems (for example, to serve as the baseline for identifying and assessing suspicious transactions on a contemporaneous basis).<sup>20</sup> Rather, FinCEN expects firms to use the customer information and customer risk profile as appropriate during the course of complying with their obligations under the BSA in order to determine whether a particular flagged transaction is suspicious.<sup>21</sup>

### Conducting Ongoing Monitoring

As with the requirement to understand the nature and purpose of the customer relationship, the requirement to conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial ownership of legal entity customers, merely adopts existing supervisory and regulatory expectations as explicit minimum standards of customer due diligence required for firms' AML programs.<sup>22</sup> If, in the course of its normal monitoring for suspicious activity, the member firm detects information that is relevant to assessing the customer's risk profile, the member firm must update the customer information, including the information regarding the beneficial owners of legal entity customers, as discussed below.<sup>23</sup> However, there is no expectation that the member firm update customer information, including beneficial ownership information, on an ongoing or continuous basis.<sup>24</sup>

### Identifying and Verifying the Identity of Beneficial Owners of Legal Entity Customers

In addition to requiring that member firms incorporate the fifth pillar into their AML programs, the CDD Rule also requires member firms to establish and maintain written procedures as part of their AML programs that are reasonably designed to identify and verify the identities of beneficial owners<sup>25</sup> of legal entity customers.<sup>26</sup> FinCEN states that this information can provide law enforcement with key details about suspected criminals who conceal illicit activity and assets through legal structures they own or control.<sup>27</sup> In addition, FinCEN states the information will help financial institutions to assess and mitigate risk more effectively in connection with existing requirements, such as enhancing suspicious activity report filings.<sup>28</sup>

Under the CDD Rule, member firms must obtain from the natural person opening the account<sup>29</sup> on behalf of the legal entity customer, the identity of the beneficial owners of the entity.<sup>30</sup> In addition, that individual must certify, to the best of his or her knowledge, as to the accuracy of the information. FinCEN intends that the legal entity customer identify its ultimate beneficial owner(s) and not “nominees” or “straw men.”<sup>31</sup> The CDD Rule does not prescribe the form in which member firms must collect the required information, which includes the name, date of birth, address and Social Security number or other government identification number of beneficial owners.<sup>32</sup> Rather, member firms may choose to obtain the information by using FinCEN’s standard certification form<sup>33</sup> adopted as part of this rulemaking or by another means, provided that the chosen method satisfies the identification requirements in the CDD Rule.<sup>34</sup> In any case, the CDD Rule requires that member firms maintain records of the beneficial ownership information they obtain.<sup>35</sup>

Once member firms obtain the required beneficial ownership information, the CDD Rule requires that member firms verify the identity of the beneficial owner(s) – in other words, that they are who they say they are and not their status as beneficial owners – through risk-based procedures that include, at a minimum, the elements required for member firms’ CIP procedures for verifying the identity of individual customers.<sup>36</sup> Such verification must be completed within a reasonable time after account opening.<sup>37</sup> Member firms may rely on the beneficial ownership information supplied by the individual opening the account, provided that they have no knowledge of facts that would reasonably call into question the reliability of that information.<sup>38</sup>

To the same extent as permitted under the CIP rules, the CDD Rule permits member firms to rely on another financial institution for the performance of the CDD Rule’s requirements.<sup>39</sup>

The CDD Rule’s requirements with respect to beneficial owners of legal entity customers applies on a prospective basis, that is, only with respect to legal entity customers that open new accounts from the date of the CDD Rule’s implementation. However, a member firm should obtain beneficial ownership information for an existing legal entity customer if, during the course of normal monitoring, it receives information that is needed to assess or reevaluate the risk of the customer.<sup>40</sup>

## Endnotes

1. 31 U.S.C. 5311, *et seq.*
2. *See* 31 U.S.C. 5312(a)(2) (defining “financial institution”).
3. 31 U.S.C. 5318(h)(1).
4. 31 CFR 1023.210(b).
5. FinCEN Customer Due Diligence Requirements for Financial Institutions; CDD Rule, 81 FR 29397 (May 11, 2016) (CDD Rule Release); 82 FR 45182 (September 28, 2017) (making technical correcting amendments to the final CDD Rule published on May 11, 2016). FinCEN is authorized to impose AML program requirements on financial institutions and to require financial institutions to maintain procedures to ensure compliance with the BSA and associated regulations. 31 U.S.C. 5318(h)(2) and (a)(2). The CDD Rule is the result of the rulemaking process FinCEN initiated in March 2012. *See* 77 FR 13046 (March 5, 2012) (Advance Notice of Proposed Rulemaking) and 79 FR 45151 (August 4, 2014) (Notice of Proposed Rulemaking).
6. *See* 31 CFR. 1010.230(f) (defining “covered financial institution”).
7. *See* CDD Rule Release at 29398.
8. On July 19, 2016, FinCEN published Frequently Asked Questions on the CDD Rule. *See* U.S. Department of the Treasury Financial Crimes Enforcement Network Guidance FIN-2016-G003, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions* (July 19, 2016) (FinCEN FAQs).
9. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).
10. If a member firm does not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (*e.g.*, engages solely in proprietary trading or conducts business only with other broker-dealers), then “independent testing” is required every two years. *See* FINRA Rule 3310(c).
11. In fact, FinCEN notes that broker-dealers must continue to comply with FINRA Rules, notwithstanding differences between the CDD Rule and FINRA Rule 3310. *See* CDD Rule Release 29421, n. 85.
12. *See* CDD Rule Release at 29420; 31 CFR 1023.210.
13. *See id.* at 29420-21.
14. *See id.* at 29419.
15. *See id.* at 29421.
16. *See id.* at 29422.
17. *See id.*
18. *See id.*
19. *See id.*
20. *See id.*
21. *See id.*
22. *See id.* at 29402.
23. *See id.* at 29420-21.
24. *See id.*

25. There are both ownership and control prongs of the definition of beneficial owner for purposes of the CDD Rule. A beneficial owner is: (1) each individual (if any) who directly or indirectly owns 25 percent of the equity interests of a legal entity customer; and (2) a single individual with significant responsibility to *control, manage, or direct* a legal entity customer, including an executive officer or senior manager. *See id.* at 29409; FinCEN FAQs Question 9; 31 CFR 1010.230(d). Despite imposing a 25 percent threshold for the ownership prong, FinCEN's guidance suggests that financial institutions may find it appropriate to identify and verify beneficial owners at a lower ownership threshold if circumstances warrant. *See* CDD Rule Release at 29410. For guidance on the types of individuals that have "significant responsibility to control, manage, or direct a legal entity customer," *see* FinCEN FAQs, Question 13.
  26. A legal entity customer is a "corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction, that opens an account." 31 CFR 1010.230(e)(1). The requirements to identify and verify the identity of beneficial owners do not apply to, among others, financial institutions regulated by a Federal functional regulator or a bank regulated by a state bank regulator, investment advisers, as defined in the Investment Advisers Act of 1940, that are registered with the Securities and Exchange Commission (SEC), entities registered with the SEC under the Securities Exchange Act of 1934, state-regulated insurance companies and specified pooled investment vehicles. For a full list of entities excluded from the legal entity customer definition, *see* 31 CFR 1010.230(e)(2).
- In addition, in the FinCEN FAQs, FinCEN stated that the definition of legal entity customer does not include sole proprietorships, unincorporated associations, trusts (other than statutory trusts) or natural persons opening the account on their own behalf. *See* FinCEN FAQs, Question 20. Furthermore, the CDD Rule clarifies who is the legal entity customer in the context of intermediated account relationship. It explains that, to the extent that existing guidance provides that, for purposes of the customer identification program (CIP) rules, a financial institution shall treat an intermediary (and not the intermediary's customers) as its customer, the financial institution should treat the intermediary as its customer for the CDD Rule. *See* CDD Rule Release at 29416.
27. *See* CDD Rule Release at 294000.
  28. *See id.*
  29. The CDD Rule incorporates the definition of "account" that is used in the CIP rules. *See* 31 CFR 1010.230(c). *See also* 31 CFR 1020.100(a)(2) (for banks); 1023.100(a)(2) (for brokers and dealers in securities); 1024.100(a)(2) (for mutual funds); and 1026.100(a)(2) (for futures commission merchants or introducing brokers in commodities). Covered financial institutions are not required to identify and verify the beneficial owners of certain entities that are excluded from the definition, and covered financial institutions that open certain types of accounts for legal entity customers do not have to verify the beneficial owners of those entities. *See* FinCEN FAQs, Questions 17, 20, 21 and 22.
  30. The natural person opening the account on behalf of the legal entity customer could be, though need not be, a beneficial owner of the legal entity customer. *See* FinCEN FAQs, Question 10.

31. *See* FinCEN FAQs, Question 1.
32. *See* FinCEN FAQs, Question 11.
33. *See* Appendix A to 31 CFR 1010.230; CDD Rule Release at 29454.
34. *See* 31 CFR 1010.230(b)(1); CDD Rule Release at 29405.
35. *See* CDD Rule Release at 29405.
36. *See id.* at 29407.
37. *See id.* at 29408.
38. *See id.* at 29407.
39. *See* 31 CFR 1010.230(i) and (j). A financial institution must have procedures for maintaining a record of information obtained in connection with identifying and verifying beneficial owners for a period of five years after the date the account is closed. *See also* Letter from Emily Westerberg Russell, Senior Special Counsel, Division of Trading and Markets, SEC, to Aseel Rabie, Managing Director and Associate General Counsel, Securities Industry and Financial Markets Association (SIFMA), dated December 12, 2016 (SIFMA SEC No-Action Letter), available at <https://www.sec.gov/divisions/marketreg/mr-noaction/2016/securities-industry-financial-markets-association-120916.pdf> (extending no action relief when broker-dealers rely on investment advisers for identifying and verifying beneficial owners of legal entity customers, subject to enumerated conditions).
40. *See id.* at 29404.

# Regulatory Notice

19-18

## Anti-Money Laundering (AML) Program

### FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations

#### Summary

FINRA is issuing this *Notice* to provide guidance to member firms regarding suspicious activity monitoring and reporting obligations under FINRA Rule 3310 (Anti-Money Laundering Compliance Program).

Questions concerning this *Notice* should be directed to:

- ▶ Victoria Crane, Associate General Counsel, Office of General Counsel, at (202) 728-8104 or [victoria.crane@finra.org](mailto:victoria.crane@finra.org); or
- ▶ Blake Snyder, Senior Director, Member Regulation, at (561) 443-8051 or [blake.snyder@finra.org](mailto:blake.snyder@finra.org).

#### Background and Discussion

FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires each member firm to develop and implement a written anti-money laundering (AML) program reasonably designed to achieve and monitor the firm's compliance with the requirements of the Bank Secrecy Act (BSA),<sup>1</sup> and the implementing regulations promulgated thereunder by the Department of the Treasury (Treasury).

FINRA Rule 3310(a) requires firms to "[e]stablish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of transactions required under [the BSA] and the implementing regulation thereunder." The BSA authorizes Treasury to require that financial institutions file suspicious activity reports (SARs).<sup>2</sup>

May 6, 2019

#### Notice Type

- ▶ Guidance

#### Suggested Routing

- ▶ Compliance
- ▶ Legal
- ▶ Operations
- ▶ Senior Management

#### Key Topics

- ▶ Anti-Money Laundering
- ▶ Compliance Programs

#### Referenced Rules & Notices

- ▶ Bank Secrecy Act
- ▶ FINRA Rule 3310
- ▶ Notice to Members 02-21



Under Treasury's SAR rule,<sup>3</sup> a broker-dealer must report a transaction to the Financial Crimes Enforcement Network (FinCEN) if it is conducted or attempted by, at or through a broker-dealer, it involves or aggregates funds or other assets of at least \$5,000, and the broker-dealer knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- ▶ involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- ▶ is designed, whether through structuring or other means, to evade any regulations promulgated under the BSA;
- ▶ has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the broker-dealer knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- ▶ involves use of the broker-dealer to facilitate criminal activity.<sup>4</sup>

Broker-dealers must report the suspicious activity by completing a SAR and filing it in accordance with the requirements of Treasury's SAR rule.<sup>5</sup> Broker-dealers must maintain a copy of any SAR filed and supporting documentation for a period of five years from the date of filing the SAR.<sup>6</sup> FinCEN has provided guidance<sup>7</sup> to the industry advising that if the activity that was the subject of a SAR filing continues, firms should review any continuing activity at least every 90 days to consider whether a continuing activity SAR filing is warranted, with the filing deadline being 120 days after the date of the previously related SAR filing.

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers must immediately notify by telephone an appropriate law enforcement authority in addition to filing timely a SAR. The firm may call FinCEN's Hotline at (866) 556-3974.

### Money Laundering Red Flags

FINRA published a list of "money laundering red flags" in [Notice to Members 02-21](#) (NTM 02-21). Since NTM 02-21 was published, guidance detailing additional red flags that may be applicable to the securities industry have been published by a number of U.S. government agencies and international organizations.<sup>8</sup> FINRA is issuing this *Notice* to provide examples of these additional money laundering red flags for firms to consider incorporating into their AML programs, as may be appropriate in implementing a risk-based approach to BSA/AML compliance. This could include, as applicable, incorporation into policies and procedures relating to suspicious activity monitoring or suspicious activity investigation



and SAR reporting. Upon detection of red flags through monitoring, firms should consider whether additional investigation, customer due diligence measures or a SAR filing may be warranted.

The following is not an exhaustive list and does not guarantee compliance with AML program requirements or provide a safe harbor from regulatory responsibility. Further, it is important to note that a red flag is not necessarily indicative of suspicious activity, and that not every item identified in this *Notice* will be relevant for every broker-dealer, every customer relationship or every business activity.

Firms should also be aware of emerging areas of risk, such as risks associated with activity in digital assets. Regardless of whether such assets are securities, BSA/AML requirements, including SAR filing requirements apply, and firms should thus consider the relevant risks, monitor for suspicious activity and, as applicable, report any such activity.

This *Notice* is intended to assist broker-dealers in complying with their existing obligations under BSA/AML requirements and does not create any new requirements or expectations. In addition, this *Notice* incorporates the red flags listed in NTM 02-21 so that firms can refer to this *Notice* only for examples of potential red flags.

#### **I. Potential Red Flags in Customer Due Diligence and Interactions With Customers**

1. The customer provides the firm with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided. Or, the customer provides information that is inconsistent with other available information about the customer. This indicator may apply to account openings and to interaction subsequent to account opening.
2. The customer is reluctant or refuses to provide the firm with complete customer due diligence information as required by the firm's procedures, which may include information regarding the nature and purpose of the customer's business, prior financial relationships, anticipated account activity, business location and, if applicable, the entity's officers and directors.
3. The customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
4. The customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (*e.g.*, known as a narcotics producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
5. The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
6. The customer has no discernable reason for using the firm's service or the firm's location (*e.g.*, the customer lacks roots to the local community or has gone out of his or her way to use the firm).

7. The customer has been rejected or has had its relationship terminated as a customer by other financial services firms.
8. The customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
9. The customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.
10. The customer is a trust, shell company or private investment company that is reluctant to provide information on controlling parties and underlying beneficiaries.
11. The customer is publicly known or known to the firm to have criminal, civil or regulatory proceedings against him or her for crime, corruption or misuse of public funds, or is known to associate with such persons. Sources for this information could include news items, the Internet or commercial database searches.
12. The customer's background is questionable or differs from expectations based on business activities.
13. The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent business or other purpose.
14. An account is opened by a politically exposed person (PEP),<sup>9</sup> particularly in conjunction with one or more additional risk factors, such as the account being opened by a shell company<sup>10</sup> beneficially owned or controlled by the PEP, the PEP is from a country which has been identified by FATF as having strategic AML regime deficiencies, or the PEP is from a country known to have a high level of corruption.
15. An account is opened by a non-profit organization that provides services in geographic locations known to be at higher risk for being an active terrorist threat.<sup>11</sup>
16. An account is opened in the name of a legal entity that is involved in the activities of an association, organization or foundation whose aims are related to the claims or demands of a known terrorist entity.<sup>12</sup>
17. An account is opened for a purported stock loan company, which may hold the restricted securities of corporate insiders who have pledged the securities as collateral for, and then defaulted on, purported loans, after which the securities are sold on an unregistered basis.
18. An account is opened in the name of a foreign financial institution, such as an offshore bank or broker-dealer, that sells shares of stock on an unregistered basis on behalf of customers.
19. An account is opened for a foreign financial institution that is affiliated with a U.S. broker-dealer, bypassing its U.S. affiliate, for no apparent business purpose. An apparent business purpose could include access to products or services the U.S. affiliate does not provide.

## II. Potential Red Flags in Deposits of Securities

1. A customer opens a new account and deposits physical certificates, or delivers in shares electronically, representing a large block of thinly traded or low-priced securities.
2. A customer has a pattern of depositing physical share certificates, or a pattern of delivering in shares electronically, immediately selling the shares and then wiring, or otherwise transferring out the proceeds of the sale(s).
3. A customer deposits into an account physical share certificates or electronically deposits or transfers shares that:
  - were recently issued or represent a large percentage of the float for the security;
  - reference a company or customer name that has been changed or that does not match the name on the account;
  - were issued by a shell company;
  - were issued by a company that has no apparent business, revenues or products;
  - were issued by a company whose SEC filings are not current, are incomplete, or nonexistent;
  - were issued by a company that has been through several recent name changes or business combinations or recapitalizations;
  - were issued by a company that has been the subject of a prior trading suspension; or
  - were issued by a company whose officers or insiders have a history of regulatory or criminal violations, or are associated with multiple low-priced stock issuers.
4. The lack of a restrictive legend on deposited shares seems inconsistent with the date the customer acquired the securities, the nature of the transaction in which the securities were acquired, the history of the stock or the volume of shares trading.
5. A customer with limited or no other assets at the firm receives an electronic transfer or journal transfer of large amounts of low-priced, non-exchange-listed securities.
6. The customer's explanation or documents purporting to evidence how the customer acquired the shares does not make sense or changes upon questioning by the firm or other parties. Such documents could include questionable legal opinions or securities purchase agreements.
7. The customer deposits physical securities or delivers in shares electronically, and within a short time-frame, requests to journal the shares into multiple accounts that do not appear to be related, or to sell or otherwise transfer ownership of the shares.
8. Seemingly unrelated clients open accounts on or at about the same time, deposit the same low-priced security and subsequently liquidate the security in a manner that suggests coordination.

**III. Potential Red Flags in Securities Trading<sup>13</sup>**

1. The customer, for no apparent reason or in conjunction with other “red flags,” engages in transactions involving certain types of securities, such as penny stocks, Regulation “S” stocks and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer’s activity.)
2. There is a sudden spike in investor demand for, coupled with a rising price in, a thinly traded or low-priced security.
3. The customer’s activity represents a significant proportion of the daily trading volume in a thinly traded or low-priced security.
4. A customer buys and sells securities with no discernable purpose or circumstances that appear unusual.
5. Individuals known throughout the industry to be stock promoters sell securities through the broker-dealer.
6. A customer accumulates stock in small increments throughout the trading day to increase price.
7. A customer engages in pre-arranged or other non-competitive securities trading, including wash or cross trades, with no apparent business purpose.
8. A customer attempts to influence the closing price of a stock by executing purchase or sale orders at or near the close of the market.
9. A customer engages in transactions suspected to be associated with cyber breaches of customer accounts, including potentially unauthorized disbursements of funds or trades.
10. A customer engages in a frequent pattern of placing orders on one side of the market, usually inside the existing National Best Bid or Offer (NBBO), followed by the customer entering orders on the other side of the market that execute against other market participants that joined the market at the improved NBBO (activity indicative of “spoofing”).
11. A customer engages in a frequent pattern of placing multiple limit orders on one side of the market at various price levels, followed by the customer entering orders on the opposite side of the market that are executed and the customer cancelling the original limit orders (activity indicative of “layering”).
12. Two or more unrelated customer accounts at the firm trade an illiquid or low-priced security suddenly and simultaneously.
13. The customer makes a large purchase or sale of a security, or option on a security, shortly before news or a significant announcement is issued that affects the price of the security.

14. The customer is known to have friends or family who work at or for the securities issuer, which may be a red flag for potential insider trading or unlawful sales of unregistered securities.
15. The customer's purchase of a security does not correspond to the customer's investment profile or history of transactions (*e.g.*, the customer may never have invested in equity securities or may have never invested in a given industry, but does so at an opportune time) and there is no reasonable explanation for the change.
16. The account is using a master/sub structure, which enables trading anonymity with respect to the sub-accounts' activity, and engages in trading activity that raises red flags, such as the liquidation of microcap issuers or potentially manipulative trading activity.
17. The firm receives regulatory inquiries or grand jury or other subpoenas concerning the firm's customers' trading.
18. The customer engages in a pattern of transactions in securities indicating the customer is using securities to engage in currency conversion. For example, the customer delivers in and subsequently liquidates American Depositary Receipts (ADRs) or dual currency bonds for U.S. dollar proceeds, where the securities were originally purchased in a different currency.
19. The customer engages in mirror trades or transactions involving securities used for currency conversions, potentially through the use of offsetting trades.
20. The customer appears to buy or sell securities based on advanced knowledge of pending customer orders.

#### **IV. Potential Red Flags in Money Movements**

1. The customer attempts or makes frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies and procedures relating to the deposit of cash and cash equivalents.
2. The customer "structures" deposits, withdrawals or purchases of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements, and may state directly that they are trying to avoid triggering a reporting obligation or to evade taxing authorities.
3. The customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
4. The customer's account shows numerous currency, money order (particularly sequentially numbered money orders) or cashier's check transactions aggregating to significant sums without any apparent business or lawful purpose.

5. The customer frequently changes bank account details or information for redemption proceeds, in particular when followed by redemption requests.
6. The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
7. Wire transfers are made in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
8. Incoming payments are made by third-party checks or checks with multiple endorsements.
9. Outgoing checks to third parties coincide with, or are close in time to, incoming checks from other third parties.
10. Payments are made by third party check or money transfer from a source that has no apparent connection to the customer.
11. Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.
12. Wire transfers originate from jurisdictions that have been highlighted in relation to black market peso exchange activities.
13. The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (*e.g.*, countries designated by national authorities, such as FATF, as non-cooperative countries and territories).
14. The parties to the transaction (*e.g.*, originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
15. Wire transfers or payments are made to or from unrelated third parties (foreign or domestic), or where the name or account number of the beneficiary or remitter has not been supplied.
16. There is wire transfer activity that is unexplained, repetitive, unusually large, shows unusual patterns or has no apparent business purpose.
17. The securities account is used for payments or outgoing wire transfers with little or no securities activities (*i.e.*, account appears to be used as a depository account or a conduit for transfers, which may be purported to be for business operating needs).
18. Funds are transferred to financial or depository institutions other than those from which the funds were initially received, specifically when different countries are involved.

19. The customer engages in excessive journal entries of funds between related or unrelated accounts without any apparent business purpose.
20. The customer uses a personal/individual account for business purposes or vice versa.
21. A foreign import business with U.S. accounts receives payments from outside the area of its customer base.
22. There are frequent transactions involving round or whole dollar amounts purported to involve payments for goods or services.
23. Upon request, a customer is unable or unwilling to produce appropriate documentation (*e.g.*, invoices) to support a transaction, or documentation appears doctored or fake (*e.g.*, documents contain significant discrepancies between the descriptions on the transport document or bill of lading, the invoice, or other documents such as the certificate of origin or packing list).
24. The customer requests that certain payments be routed through nostro<sup>14</sup> or correspondent accounts held by the financial intermediary instead of its own accounts, for no apparent business purpose.
25. Funds are transferred into an account and are subsequently transferred out of the account in the same or nearly the same amounts, especially when the origin and destination locations are high-risk jurisdictions.
26. A dormant account suddenly becomes active without a plausible explanation (*e.g.*, large deposits that are suddenly wired out).
27. Nonprofit or charitable organizations engage in financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
28. There is unusually frequent domestic and international automated teller machine (ATM) activity.
29. A person customarily uses the ATM to make several deposits into a brokerage account below a specified BSA/AML reporting threshold.
30. Many small, incoming wire transfers or deposits are made using checks and money orders that are almost immediately withdrawn or wired out in a manner inconsistent with the customer's business or history; the checks or money orders may reference in a memo section "investment" or "for purchase of stock." This may be an indicator of a Ponzi scheme or potential funneling activity.
31. Wire transfer activity, when viewed over a period of time, reveals suspicious or unusual patterns, which could include round dollar, repetitive transactions or circuitous money movements.

**V. Potential Red Flags in Insurance Products**

1. The customer cancels an insurance contract and directs that the funds be sent to a third party.
2. The customer deposits an insurance annuity check from a cancelled policy and immediately requests a withdrawal or transfer of funds.
3. The customer cancels an annuity product within the free-look period. This could be a red flag if accompanied with suspicious indicators, such as purchasing the annuity with several sequentially numbered money orders or having a history of cancelling annuity products during the free-look period.
4. The customer opens and closes accounts with one insurance company, then reopens a new account shortly thereafter with the same insurance company, each time with new ownership information.
5. The customer purchases an insurance product with no concern for the investment objective or performance.

**VI. Other Potential Red Flags**

1. The customer is reluctant to provide information needed to file reports to proceed with the transaction.
2. The customer exhibits unusual concern with the firm's compliance with government reporting requirements and the firm's AML policies.
3. The customer tries to persuade an employee not to file required reports or not to maintain the required records.
4. Notifications received from the broker-dealer's clearing firm that the clearing firm had identified potentially suspicious activity in customer accounts. Such notifications can take the form of alerts or other concern regarding negative news, money movements or activity involving certain securities.
5. Law enforcement has issued subpoenas or freeze letters regarding a customer or account at the securities firm.
6. The customer makes high-value transactions not commensurate with the customer's known income or financial resources.
7. The customer wishes to engage in transactions that lack business sense or an apparent investment strategy, or are inconsistent with the customer's stated business strategy.
8. The stated business, occupation or financial resources of the customer are not commensurate with the type or level of activity of the customer.
9. The customer engages in transactions that show the customer is acting on behalf of third parties with no apparent business or lawful purpose.



10. The customer engages in transactions that show a sudden change inconsistent with normal activities of the customer.
11. Securities transactions are unwound before maturity, absent volatile market conditions or other logical or apparent reason.
12. The customer does not exhibit a concern with the cost of the transaction or fees (*e.g.*, surrender fees, or higher than necessary commissions).
13. A borrower defaults on a cash-secured loan or any loan that is secured by assets that are readily convertible into currency.
14. There is an unusual use of trust funds in business transactions or other financial activity.

## Endnotes

1. 31 U.S.C. 5311, *et seq.*
2. *See* 31 U.S.C. 5318(g).
3. *See* 31 CFR 1023.320.
4. *See* 31 CFR 1023.320(a)(2).
5. *See* 31 CFR 1023.320.
6. *See* 31 CFR 1023.320(d).
7. *See* [FinCEN SAR Activity Review Issue 21](#) (May 2012).
8. *See, e.g.*, Financial Action Task Force (FATF), [Guidance for a Risk-Based Approach for the Securities Sector](#), October 2018; FATF, [Money Laundering and Terrorist Financing in the Securities Sector](#), October 2009; FATF, [Guidance for Financial Institutions in Detecting Terrorist Financing](#), April 2002; FATF Report, [Laundering the Proceeds of Corruption](#), July 2011; FATF Report, [Risk of Terrorist Abuse in Non-Profit Organisations](#), June 2014; [FinCEN Advisory FIN-2010-A001: Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade Based Money Laundering](#), February 2010; U.S. Department of State, [Money Laundering Methods, Trends and Typologies](#), March 2004; Securities and Exchange Commission (SEC) [National Exam Risk Alert on Master/Sub-accounts](#), September 2011; SEC [National Exam Risk Alert on Broker-Dealer Controls Regarding Customer Sales of Microcap Securities](#), October 2014; and SEC [Responses to Frequently Asked Questions about a Broker-Dealer's Duties When Relying on the Securities Act Section 4\(a\)\(4\) Exemption to Execute Customer Orders](#), October 2014. *See also* [Regulatory Notices 09-05](#) (January 2009) and [10-18](#) (April 2010); and [Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering, Money Laundering and Terrorist Financing "Red Flags."](#)
9. A "Politically Exposed Person" is defined by FATF as an individual who is or has been entrusted with a prominent public function, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, or important political party officials. *See* FATF Guidance, [Politically Exposed Persons](#), June 2013.
10. A "shell company" is an issuer of securities for which a registration statement has been filed with the SEC that has: (1) no or nominal operations; and (2) either: (i) no or nominal assets; (ii) assets consisting solely of cash and cash equivalents; or (iii) assets consisting of any amount of cash or cash equivalents and nominal other assets. *See* 17 CFR 230.504.
11. The FATF Report on [Risk of Terrorist Abuse in Non-Profit Organisations](#) (FATF Report), June 2014, defines "terrorist threat" as: A person or group of people, object or activity, with the potential to cause harm. Threat is contingent on actors that possess both the capability and intent to do harm.
12. The FATF Report defines "terrorist entity" as a terrorist and/or terrorist organization identified as a supporter of terrorism by national or international sanctions lists, or assessed by a jurisdiction as active in terrorist activity. *See id.*
13. These red flags could also be indicative of securities law violations.
14. Nostro accounts are accounts that a financial institution holds in a foreign currency in another bank, typically in order to facilitate foreign exchange transactions.

# Regulatory Notice

20-13

## Heightened Threat of Fraud and Scams

### FINRA Reminds Firms to Beware of Fraud During the Coronavirus (COVID-19) Pandemic

#### Summary

The COVID-19 pandemic is affecting most aspects of our society and daily lives, as well as the U.S. economy and markets. Events with such profound impact routinely create opportunities for financial fraud.

Firms and their associated persons should be aware of and take appropriate measures to address the increased risks and challenges presented during the COVID-19 pandemic. In addition to new scams focusing on COVID-19, previous scams may also find new life as fraudsters adapt to and exploit recent events and related vulnerabilities, especially those related to the remote working environment.

FINRA is committed to providing guidance, updates and other information to help stakeholders stay informed about the latest developments relating to COVID-19, which can be found on FINRA's [COVID-19/Coronavirus Topic Page](#).

FINRA will also continue to inform the industry on emerging cybersecurity trends and related frauds, and reminds firms to review resources on [FINRA's Cybersecurity Topic Page](#), which provides information on how firms can strengthen their cybersecurity programs.

Questions regarding this *Notice* should be directed to:

- ▶ Greg Ruppert, Executive Vice President, National Cause and Financial Crimes Detection Programs, Member Supervision, at (415) 217-1120 or [greg.ruppert@finra.org](mailto:greg.ruppert@finra.org); or
- ▶ Sam Draddy, Senior Vice President, Insider Trading and PIPEs Surveillance, Member Supervision, at (240) 386 5042 or [sam.draddy@finra.org](mailto:sam.draddy@finra.org).

#### Background and Discussion

FINRA urges firms and associated persons to be cognizant of the heightened threat of frauds and scams to which firms and their customers may be exposed during the COVID-19 pandemic. This *Notice* outlines four common scams—(1) fraudulent account openings and money transfers; (2) firm

May 5, 2020

#### Notice Type

- ▶ Special Alert

#### Suggested Routing

- ▶ AML
- ▶ Compliance
- ▶ Cybersecurity
- ▶ Financial Crimes Department
- ▶ Fraud Department
- ▶ Legal
- ▶ New Accounts
- ▶ Operations
- ▶ Registered Representatives
- ▶ Risk Management
- ▶ Senior Management

#### Key Topics

- ▶ Cybersecurity
- ▶ Fraud

#### Referenced Rules and Notices

- ▶ FINRA Rule 2090
- ▶ FINRA Rule 3110
- ▶ FINRA Rule 3310
- ▶ FINRA Rule 4512
- ▶ Information Notice 3/26/20
- ▶ Information Notice 4/29/19
- ▶ Regulatory Notice 09-64
- ▶ Regulatory Notice 12-05
- ▶ Regulatory Notice 19-18

imposter scams; (3) IT Help Desk scams; and (4) business email compromise schemes—and describes measures that firms and associated persons may take to mitigate related risks. This information pre-dates the COVID-19 pandemic but may be useful to firms since FINRA has observed that these threats persist in the current environment.

## I. Fraudulent Account Openings and Money Transfers

Some firms have reported an increase in newly opened fraudulent accounts, which may otherwise be hard to identify as a result of overall increases in new account openings. Firms should be aware that fraudsters are targeting firms offering online account opening and, perhaps especially, firms that recently started offering such services. These fraudsters may be taking advantage of the pandemic to use stolen or synthetic identities to establish accounts to divert congressional stimulus funds, unemployment payments or to engage in automated clearing house (ACH) fraud.<sup>1</sup>

### Common Characteristics of Scams

The specific tactics fraudsters use may vary, but they typically involve some combination of the following steps:

- ▶ **Establishing the Account**—Using stolen or synthetic customer identity information to establish a new brokerage account;<sup>2</sup>
- ▶ **Funding the Account**—Funding the newly established brokerage account by:
  - ▶ using stolen bank account information (routing and account numbers) to transfer money from the customer's bank account to the newly established brokerage account;
  - ▶ effecting smaller dollar transfers via ACH or other online payment methods from the customer's bank account; or
  - ▶ diverting other customer funds directly to the fraudster's account (*e.g.*, diverting unemployment benefits); and
- ▶ **Exfiltrating Funds**—Rapidly moving deposited funds out of the brokerage account by, for example:
  - ▶ making ATM withdrawals or purchases on debit cards for the brokerage account; or
  - ▶ linking the brokerage account to a third-party bank account or an account at another financial institution that provides pre-paid debit card products and services and then transferring funds to that account.

FINRA has observed that, in some cases, fraudsters emailed firms a falsified voided check to verify the new bank account information. The falsified check included the real customer's home address and looked like a legitimate check for the customer's bank account.

### Selected Firm Practices

FINRA has observed firms implement the following practices to address risks relating to fraudulent account openings and money transfers:

- ▶ **Customer Identification Program<sup>3</sup>**—Firms that permitted the opening of accounts through electronic means used both documentary and non-documentary methods to verify the identity of customers, including:
  - ▶ documentary identification (which included unexpired government-issued identification bearing a photograph, such as drivers' licenses or passports); and
  - ▶ non-documentary methods (which included contacting the customer; independently verifying the customer's identity with information obtained from a consumer reporting agency, public database or other source; checking references with other financial institutions; or obtaining a financial statement).
- ▶ **Monitoring for Fraud During Account Opening**—Firms used the following methods at the time of account opening to identify potential fraud:
  - ▶ limiting automated approval of multiple accounts opened by a single customer;
  - ▶ reviewing account application fields—such as telephone number, address, email address, bank routing numbers and account numbers—for repetition or commonalities among multiple applications, but with different customer names or identifiers; and
  - ▶ using technology to detect indicators of automated scripted attacks in the digital account application process (*e.g.*, extremely rapid completion of account applications).

Although some firms use micro-deposits as a mean to verify accounts, FINRA notes that other firms are concerned that fraudsters can undermine the utility of this verification method by using social engineering attacks to take over customer accounts at institutions across the financial services industry. As a result, and as discussed further below, these firms carefully watch for rapid withdrawals from accounts that were verified using micro-deposits.

- ▶ **Bank Account Verification and Restrictions on Fund Transfers**—Firms confirmed customers' identities with banks and restricted fund transfers in certain situations by, for example:
  - ▶ reviewing the IP address of transfer requests made online or through a mobile device to determine if the request was made from a location that is consistent with the customer's home address or locations from which the firm has previously received legitimate customer communications;

- ▶ verifying that the identity on the source account for fund transfers matches the customer's identity at the broker-dealer;
  - ▶ confirming that the identity of the destination bank account for cash transfers matches the customer's identity at the broker-dealer;
  - ▶ prohibiting the rapid transfer of recently deposited customer funds from customers' brokerage accounts to third party bank accounts (where some firms used risk criteria—*e.g.*, the amount of the transfer in dollar terms—to trigger reviews of transfer requests) by requiring a holding period (which allowed time for the filing of an ACH fraud report by the originating bank);
  - ▶ implementing a process for customers to obtain exceptions to these restrictions, which required them to complete additional steps to verify their account information, the transfer amount and their identity (such as through the use of third-party providers that leverage customers' credit bureau or other information); and
  - ▶ creating notifications for changes to bank account information that were sent to the customer via email, text message or instant message—as well as their official street address of record—informing them about the newly established linked bank account and asking them to call the firm if they have any questions.
- ▶ **Ongoing Monitoring of Accounts**—Firms continued to evaluate existing accounts for fraud risks where the accounts:
- ▶ were inactive, unfunded and soon to be restricted or closed; and
  - ▶ had losses related to credit extensions and were about to be placed into collections or write-off categories.
- ▶ **Collaborating with Clearing Firms**—Firms clearly understood the allocation of responsibilities between clearing and introducing firms for handling ACH transactions and implemented policies and procedures to meet those responsibilities effectively, including:
- ▶ defining how instructions related to ACH requests should be conveyed; and
  - ▶ understanding the responsible staff at the introducing firm who were authorized to transmit instructions to the clearing firm.
- ▶ **Suspicious Activity Report (SAR) Filing Requirements<sup>4</sup>**—Firms confirmed that ACH fraud was covered by their SAR procedures and reported them to the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN).

### Relevant Regulatory Obligations

In addition to considering the practices noted above, FINRA encourages firms to assess their compliance programs relating to account opening and money transfers and reminds them to review their policies and procedures related to:

- ▶ new account openings to confirm they comply with FINRA Rules [2090](#) (Know Your Customer) and [4512](#) (Customer Account Information), as well as the Bank Secrecy Act and its implementing regulations addressed under FINRA Rule [3310](#) (Anti-Money Laundering Compliance Program);
- ▶ handling of ACH transfer requests to “determine the authenticity of transmittal instructions”<sup>5</sup> obligations pursuant to FINRA Rule [3110](#) (Supervision);
- ▶ safeguarding customer “records and information” pursuant to Regulation S-P Rule 30;<sup>6</sup> and
- ▶ filing SARs with FinCEN.<sup>7</sup>

### Firm Imposter Scams

The expanded use of remote offices and telework arrangements may increase opportunities for fraudsters to impersonate firms and associated persons in communicating with customers or creating a fake online presence or websites.<sup>8</sup> As part of this scam, fraudsters may seek to obtain—via a website, email, text or other communications—customers’ personal information, including account information, or trick them into making investments or transferring funds. In some cases, fraudsters may seek to reduce the likelihood that customers will realize they have been the target of a fraud by directing them not to contact the firm by phone due to long wait times.

FINRA has observed firms using a variety of methods to address risks related to imposter scams, including:

- ▶ providing staff with training or fraud alerts describing firm imposter scams and the steps associated persons can take to protect the firm and its customers;
- ▶ alerting customer-facing staff that fraudsters may use the increase in remote work to engage in social engineering schemes against associated persons and advise them to vet incoming calls purporting to be from known customer numbers—for example by arranging a video call or asking customers questions where only the customers and their registered representative would know the answer; and
- ▶ implementing the practices discussed in FINRA [Information Notice 4/29/19](#) when they become aware of imposter websites.

### IT Help Desk Scams

Remote work arrangements also may increase the opportunity for social engineering attacks involving firms' IT Help Desks. In one variant of these attacks, fraudsters pose as associated persons and contact a firm's IT Help Desk to, for example, request a password reset. The fraudsters may use the conversation with the IT Help Desk staff to gain information about a firm's technical infrastructure or business operations, which they subsequently use to attack the firm, for example, by infiltrating the firm's network and possibly stealing funds from the firm.<sup>9</sup>

FINRA has observed firms address risks relating to such scams by training their IT Help Desk staff to verify callers' identities by, for example, asking for employees' identification numbers or other firm-specific information that would be challenging for fraudsters to obtain.

In a second variant of these attacks, fraudsters pose as a member of a firm's IT Help Desk team and contact associated persons in an attempt to harvest user credentials or introduce malware into the associated person's computer, which may then be used to steal credentials, confidential customer or firm data or other valuable information.

FINRA has observed firms address this risk by training associated persons to take extra precautions when receiving unsolicited calls or emails that appear to come from their firm's IT Help Desk, especially if the caller or email asks the associated person to click a link, enter a web address or download software to their computer. Some firms ask employees receiving such calls or emails not to respond and to call back the IT Help Desk on its official number to confirm the veracity of the original communication. In addition, they ask employees to report any suspicious activity to the firm so it can alert other staff that they may be targeted.

### II. Business Email Compromise Schemes<sup>10</sup>

Fraudsters may also take advantage of remote working environments to pose, via email or text message, as firm leadership to request one or more fund transfers, for example, related to accounts payable invoices. In another variant on this scam—the gift card procurement scam—fraudsters purporting to be a manager or executive email a subordinate with an urgent request for them to secretly purchase gift cards as a motivational award or one-time surprise for staff.



FINRA has observed firms addressing such risks by alerting staff that can disburse firm funds to:

- ▶ monitor for potential red flags of scams, such as requests arriving at an unusual time of day, using atypical language or greetings, requesting a transfer to a new account, requiring privacy or secrecy for the transactions or displaying unusual urgency; and
- ▶ confirm the request via telephone prior to acting on any requests, especially those sent via email channels.

FINRA has also observed firms address such risks by including an “external” banner to highlight emails received from outside the firm.

### Reporting Fraud

Although there may not be a regulatory requirement to report every incident described in this Notice, FINRA urges firms to protect customers and other firms by immediately reporting scams and any other potential fraud to:

- ▶ FINRA’s [Regulatory Tip Form](#) found on [FINRA.org](#) or through [FINRA’s Whistleblower Tip Line](#) at (866) 96-FINRA or [whistleblower@finra.org](mailto:whistleblower@finra.org);
- ▶ U.S. Securities and Exchange Commission’s tips, complaints and referral system ([TCRs](#)) or by phone at (202) 551-4790;
- ▶ the Federal Bureau of Investigation’s (FBI) tip line at 800-CALLFBI (225-5324) or a local FBI office;
- ▶ for cyber crimes, the [Internet Crime Compliant Center \(IC3\)](#) (particularly if a firm is trying to recall a wire transfer to a destination outside the United States); and
- ▶ local state securities regulators.<sup>11</sup>

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers *must* immediately notify by telephone an appropriate law enforcement authority in addition to filing a timely SAR. The firm may call FinCEN’s Hotline at (866) 556-3974.

## Endnotes

1. A synthetic identity includes legitimate Social Security numbers (SSNs) with false names, addresses and dates of birth. Without a clearly identifiable victim, it may go undetected for longer periods of time.
2. In some cases, fraudsters have also established a new account at a firm where a legitimate customer already has an account and used at least some elements of that customer's identity to establish the new account.
3. See 31 C.F.R. 1023.220 (setting forth requirements for customer identification programs for broker-dealers).
4. See 31 C.F.R. 1023.320 (setting forth SARs reporting requirements).
5. See [Regulatory Notice 12-05](#) (Verification of Email Instructions to Transmit or Withdraw Assets From Customer Accounts) and [Regulatory Notice 09-64](#) (Customer Assets).
6. Rule 30 under Regulation S-P requires firms 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. Regulation S-P also requires firms to provide initial and annual privacy notices to customers describing information sharing policies and informing customers of their right to opt-out of information sharing. Further, FINRA Rule [3110](#) (Supervision) requires firms to establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable securities laws and regulations, including Rule 30 under Regulation S-P, and with applicable FINRA rules.
7. See [Regulatory Notice 19-18](#) (FINRA Provides Guidance to Firms Regarding Suspicious Activity Monitoring and Reporting Obligations).
8. See FINRA [Information Notice 4/29/19](#) (Imposter Websites Impacting Member Firms).
9. See FINRA [Information Notice 3/26/20](#) (Measures to Consider as Firms Respond to the Coronavirus Pandemic (COVID-19)).
10. See [FBI Release: FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic](#) (April 6, 2020).
11. See [www.nasaa.org/contact-your-regulator/](http://www.nasaa.org/contact-your-regulator/) (providing contact information for state securities regulators).

# Regulatory Notice

20-30

## Imposter Registered Representative Websites

### Fraudsters Using Registered Representatives Names to Establish Imposter Websites

#### Summary

Several firms have recently informed FINRA that malicious actors are using registered representatives' names and other information to establish websites ("imposter websites") that appear to be the representatives' personal sites and are also calling and directing potential customers to use these imposter websites. Imposters may be using these sites to collect personal information from the potential customers with the likely end goal of committing financial fraud.<sup>1</sup> This *Notice* describes certain common characteristics of these sites and actions firms and registered representatives can take to monitor for and address these sites.

Questions concerning this *Notice* should be directed to David Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or by [email](#).

#### Background and Discussion

Recently, several member firms have notified FINRA that they are observing fraudsters using registered representatives' names and other legitimate information to establish imposter websites. (See Attachment A for sample screen shots of such sites.) In addition, FINRA has received reports that the fraudsters are calling and directing potential customers to the imposter websites.

Common features of these websites include the following:

- ▶ using the registered representative's name as the domain name for the website (e.g., firstnamemiddlename.lastname.com);<sup>2</sup>
- ▶ including a picture purporting to be the registered representative;
- ▶ providing information about the registered representative's employment history, including prior employers' CRD numbers and examination history; and
- ▶ asking individuals to fill out a contact form with the individuals' names, email addresses, phone numbers, the subject of the inquiry and space for a message.

August 20, 2020

#### Notice Type

- ▶ Special Alert

#### Suggested Routing

- ▶ Legal
- ▶ Legal and Compliance
- ▶ Risk Management
- ▶ Senior Management

#### Key Topics

- ▶ Cybersecurity
- ▶ Fraud
- ▶ Imposter websites

In addition, some of the sites contain poor grammar, misspellings, odd or awkward phrasings, or misuse financial services terminology.

In addition, it is possible malicious actors could leverage the domain to send fake emails purporting to be from the registered representative and which may include imbedded phishing links or attachments containing malware.

Member firms and registered representatives can take steps to identify these pages by conducting periodic web searches using registered representatives' names. In addition, some search engines allow users to create alerts that automatically search for defined terms (*e.g.*, a registered representative's name) and inform the user of new activity.

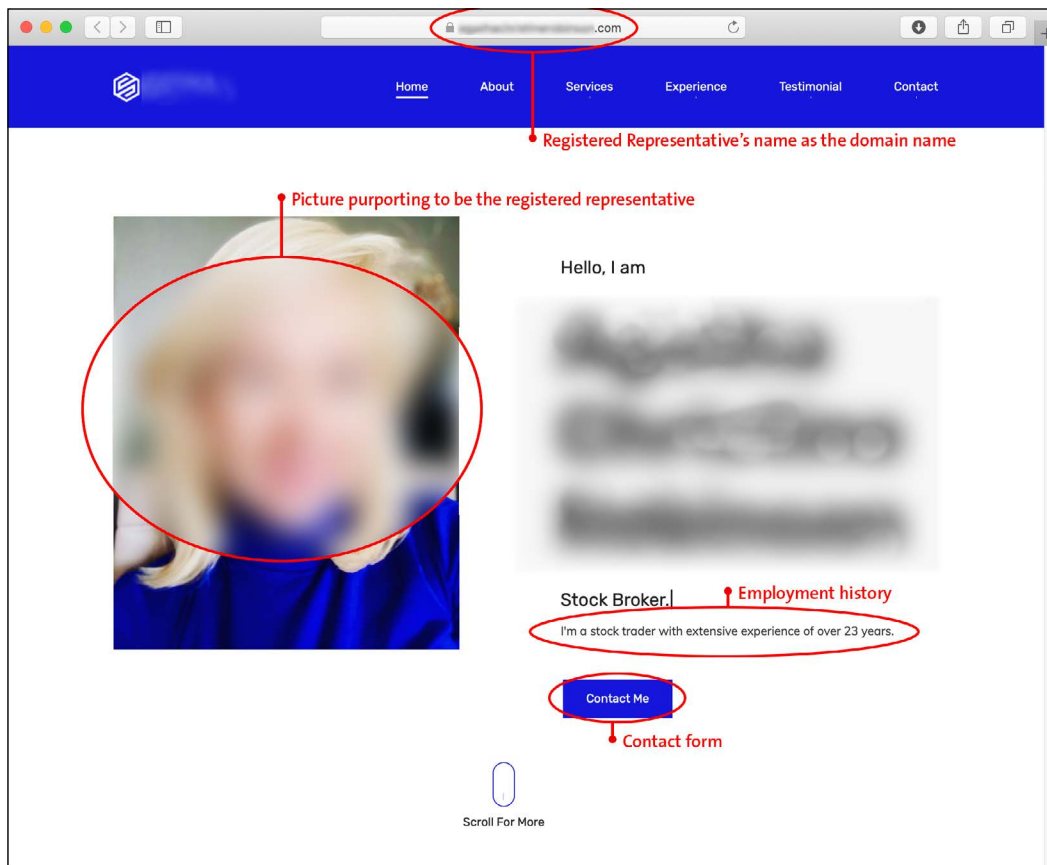
Firms may also consider the following steps similar to those FINRA noted last year in connection with risks relating to firm imposter websites:

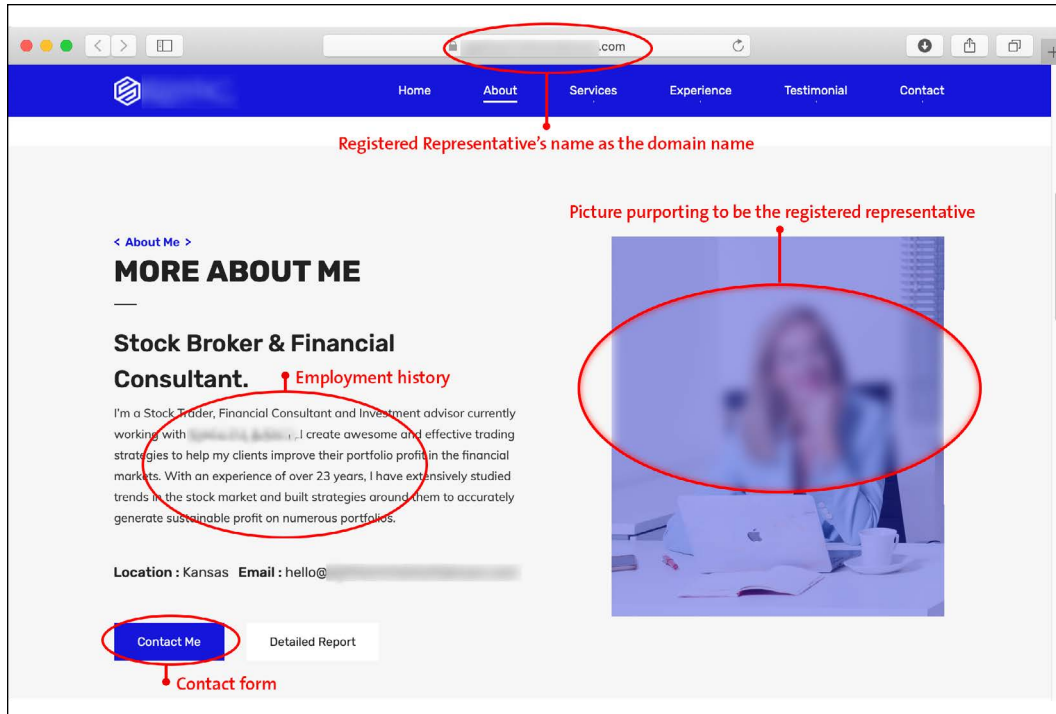
- ▶ Report the attack to the nearest Federal Bureau of Investigation (FBI) field office or the FBI's Internet Crime Complaint Center, and the relevant state's Attorney General via their websites or, if possible, a phone call.<sup>3</sup>
- ▶ Run a "WHOis" search ([www.whois.net](http://www.whois.net)) on the site to determine the hosting provider and domain name registrar associated with the imposter website (which may be the same organization in some instances). In some cases, this site also provides relevant contact information.
- ▶ Submit an abuse report to the hosting provider or the domain registrar asking them to take down the imposter website. Continue to engage with the providers by phone or email until the matter is resolved.
- ▶ Seek the assistance of a cybersecurity specialist, attorney or consultant who has experience with this type of fraud.
- ▶ Notify the U.S. Securities and Exchange Commission (SEC), FINRA or other securities or financial regulators.
- ▶ Consider posting an alert about the imposter website and the associated URL on your website, notifying registered representatives and alerting clients—especially those of the registered representative whose name is being misused—to the imposter website and also warning them not to open emails from that domain name.

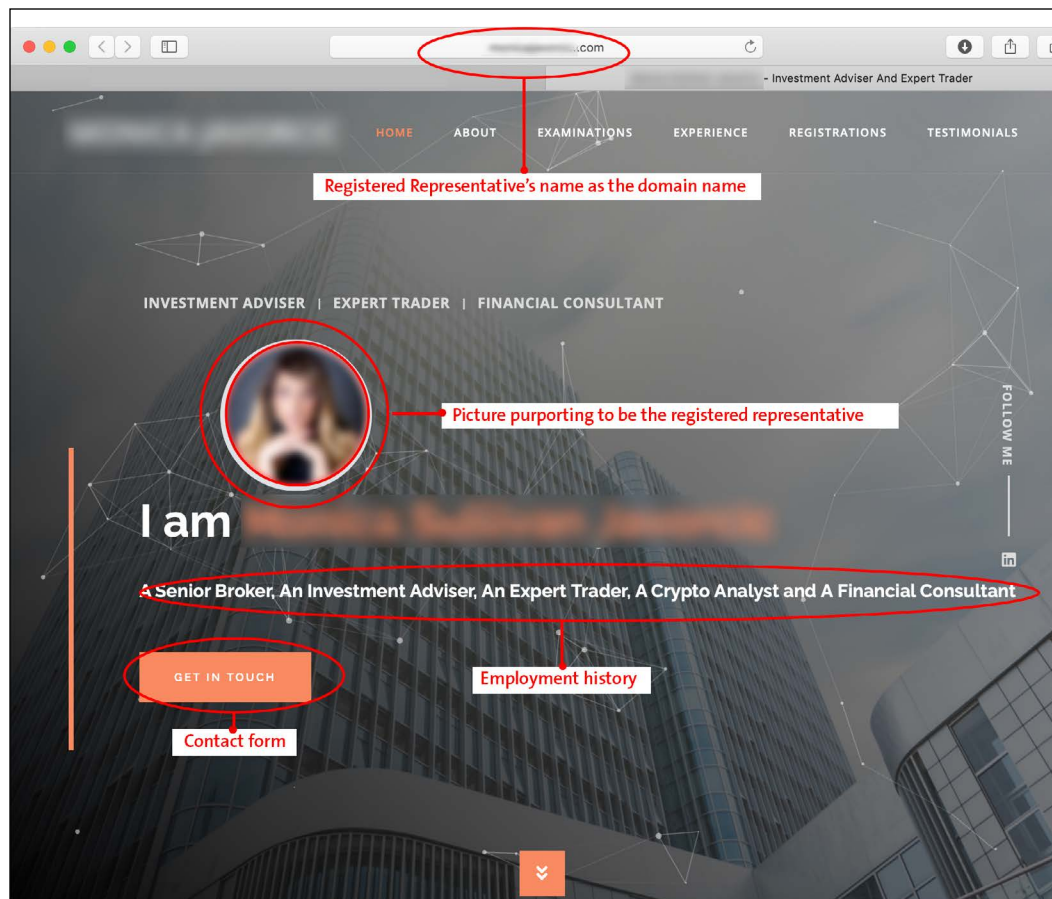
## Endnotes

1. FINRA issued [\*Information Notice 4/29/19\*](#) last year to alert firms of imposter websites targeting firms.
2. The websites reported to FINRA to date use the correct spelling of the representative's name unlike some of the imposter firm websites FINRA observed last year that sometimes used common misspellings of a name or visually similar character substitutions.
3. Member firms should consider proactively reaching out to these authorities to establish a relationship. A pre-established relationship can help facilitate the reporting and resolution process when a member firm experiences an attack.

## Attachment A









# Fraudsters Posing as Brokers or Investment Advisers – Investor Alert

**July 27, 2021**

*The FBI Criminal Investigative Division and the United States Securities and Exchange Commission's Office of Investor Education and Advocacy (OIEA) warn of fraudsters swindling investors while pretending to be registered brokers or investment advisers.*

Fraudsters may falsely claim to be registered with the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA) or a [state securities regulator](#) in order to lure investors into scams, or even impersonate real investment professionals who actually are registered with these organizations. Fraudsters may misappropriate the name, address, registration number, logo, photo, or website likeness of a currently or previously registered firm or investment professional. They try to trick investors into believing that they are registered by using a number of tactics, including the following:

- **“Spoofed Websites.”** Fraudsters may set up websites using URL addresses or names similar to those of registered firms or investment professionals to trick investors into believing that the fraudsters are registered or that the fraudsters are affiliated with a registered firm or investment professional.
- **Fake Profiles on Social Media.** Fraudsters may set up profiles impersonating registered investment professionals on popular social media platforms and then message investors to solicit their money.
- **Cold Calling.** Fraudsters may set up [boiler rooms](#) with teams of people cold calling investors to solicit their money while claiming to be employees of registered firms. The fraudsters may use technology to make it appear they are calling from the firm's location.
- **Misrepresenting or Falsifying Documents.** Fraudsters may recruit investors by misrepresenting that their firm was registered with the SEC, including pointing to the firm's [Form D](#) filings to support the misrepresentation (to learn more, read this OIEA [Investor Alert](#)). Fraudsters may solicit investors by impersonating a registered investment professional and generating a fake version of a public report using the professional's name and [CRD](#) number (to learn more, read this FINRA [Investor Alert](#)).

**Registration of Investment Professionals.** Many sellers of investment products or services are either [brokers](#), [investment advisers](#), or both. Most brokers must register with the SEC and join FINRA. Investment advisers that provide investment advice to retail investors generally must register with the SEC or the state securities regulator where they have their principal place of business.

Verify the identity of anyone offering you an investment. Don't rely on the website or contact information the person provides you. ***If you suspect someone is falsely claiming to be registered with the SEC, do not give the person any money and do not share your personal information. Report the person to the SEC.***

To quickly and easily check if someone offering you an investment is currently licensed or registered, use the search tool on [Investor.gov](#). Once you confirm that the seller is licensed or registered, make sure you are not dealing with an imposter. Contact the seller using contact information you verify independently – for example, by

using a phone number or website listed in the firm's Client Relationship Summary ([Form CRS](#)) – rather than relying on contact information the seller provides you. To ensure you are looking at a genuine copy of the firm's Form CRS, follow these steps:

1. In the "Check Out Your INVESTMENT PROFESSIONAL" search box on [Investor.gov](#), select "Firm" from the drop down options and type in the name of the firm.
2. In the search results, click on the relevant firm and then click on "Get Details."
3. Click on "Relationship Summary" or "Part 3 Relationship Summary."

For additional information about Form CRS, visit [investor.gov/CRS](#).

## Watch Out for Red Flags

Regardless of whether someone claims to be registered with the SEC, beware if you spot these warning signs of an investment scam:

- **Guaranteed High Investment Returns.** Promises of high investment returns – often accompanied by a guarantee of little or no risk – is a classic sign of fraud. Every investment has risk, and the potential for high returns usually comes with high risk.
- **Unsolicited Offers.** Unsolicited offers (you didn't ask for it and don't know the sender) to earn investment returns that seem "too good to be true" may be part of a scam.
- **Red flags in Payment Methods for Investments.**
  - **Credit Cards.** Most licensed and registered investment firms do not allow their customers to use [credit cards](#) to invest.
  - **Digital Asset Wallets and "Cryptocurrencies."** Licensed and registered financial firms typically do not require their customers to use digital asset wallets or digital assets, including so-called "cryptocurrencies," to invest.
  - **Wire Transfers and Checks.** If you pay for an investment by wire transfer or check, be suspicious if you're being asked to send or to make the payment out to a person or to a different firm, the address is suspicious (for example, an online search for the address suggests it is not an office building where the firm operates), or you are told to note that the payment is for a purpose unrelated to the investment (for example, medical expenses or a loan to a family member). ***If you wire money outside of the United States for an investment that turns out to be a scam, you likely will never see your money again.***

Report possible securities fraud to the SEC at [www.sec.gov/tcr](#). Report online fraud to the FBI's Internet Crime Complaint Center at [https://www.ic3.gov](#).

The SEC maintains a list of [Impersonators of Genuine Firms](#). This list is not exhaustive – firms may be impersonated even if they are not on the list.

FINRA staff issued an article about [imposter schemes](#).

More information about online frauds and investment scams can be found at [www.fbi.gov](#) or [Investor.gov](#), the SEC's website for individual investors.

You can contact the SEC's Office of Investor Education and Advocacy (OIEA) by phone at 1-800-732-0330, using this [online form](#), or via email at [Help@SEC.gov](#).

Receive Investor Alerts and Bulletins from OIEA by [email](#) or [RSS feed](#). Follow OIEA on [Twitter](#) @SEC\_Investor\_Ed. Like OIEA on [Facebook](#) at [facebook.com/secinvestoreducation](#).

This alert represents the views of the staff of the Office of Investor Education and Advocacy. It is not a rule, regulation, or statement of the Securities and Exchange Commission ("Commission"). The Commission has

neither approved nor disapproved its content. This bulletin, like all staff guidance, has no legal force or effect: it does not alter or amend applicable law, and it creates no new or additional obligations for any person.

*Modified: July 27, 2021*