Regulatory Notice 20-13

Heightened Threat of Fraud and Scams

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

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 4511
- Information Notice 3/26/20
- Information Notice 4/29/19
- Regulatory Notice 09-64
- Regulatory Notice 12-05
- Regulatory Notice 19-18

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*; or
- Sam Draddy, Senior Vice President, Insider Trading and PIPEs Surveillance, Member Supervision, at (240) 386 5042 or *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

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.[1]

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;[2]
- **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**[3]—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**[4]—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"[5] obligations pursuant to FINRA Rule 3110 (Supervision);
- safeguarding customer "records and information" pursuant to Regulation S-P Rule 30;[6] and
- filing SARs with FinCEN.[7]

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.[8] 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.[9]

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[10]

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*;
- 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.[11]

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/* (providing contact information for state securities regulators).