BCLP. Client Intelligent

Insights

FINRA REMINDS BROKER-DEALERS OF THEIR OBLIGATIONS TO SAFEGUARD CUSTOMER INFORMATION AND TO BUILD CONTROLS DESIGNED TO PROTECT CUSTOMERS FROM FRAUD

May 26, 2021

Key Takeaways:

- According to FINRA, the number of reported instances involving broker-dealer fraudulent account takeovers (ATO) and related theft is on the rise.
- As set forth in recently released FINRA Regulatory Notice 21-18 (“Notice 21-18"), FINRA reminds member firms of their continued obligation to safeguard customer information and to build controls designed to mitigate against fraud.
- Without creating new rules, regulations, or interpretations thereof, Notice 21-18 offers some helpful insight into some of the best practices that member firms are utilizing as of late in an effort to mitigate against the rising fraud risks.
- At the conclusion of this alert, we offer some additional best practices for member firms to consider in their compliance programs based on our own experiences with fraudulent investigations and regulatory matters.

Mobile and Online Banking Creates New Challenges in the Control Environment

Ready or not, the financial services industry is rapidly changing through innovations in technology. Accordingly, it is challenging for all broker-dealers, regardless of size or business model, to keep up with customer expectations, while at the same time protecting investors from fraud. As the industry has evolved away from the traditional telephone communications exchanged by financial advisors and their respective clients into a transactional environment driven more by online and mobile applications, there are countless ways for fraudsters to take advantage of the rapid changes in technology.

Below are several common examples of how fraudsters attempt to misappropriate and utilize customer information:

- Dark Web – Fraudsters anonymously purchase personal identifying information about brokerage customers online, including account numbers and passwords.
- Hacking – The practice of gaining unauthorized access to an investor's or firm's computer systems.
- Phishing – The practice of sending e-mails or similar communications from what appears to be reputable companies or sources asking for personal information such as social security numbers, driver's license numbers, credit card numbers, account numbers, passwords or similar information.
- Spoofing – Similar to phishing, the practice of disguising the origin of a communication in order to lure an individual into sending personal information.
- Romance Scams – Often directed at senior divorcees or widows, the practice of appealing to one's affection and trust to manipulate and steal.
- Baiting – Involves the use of a false promises for the purpose of manipulating someone into releasing information or funds.
- Ransomware or Scareware – Involves a victim being faced with false alarms and fictitious threats whereby the fraudster seeks confidential information, account numbers, or even funds, often requiring a degree of urgency on the part of the victim.
- Malware – Involves installing software or a program on a victim's computer designed to steal information.

Member Firms' Continued Regulatory Obligations

Despite the many challenges created by the rise in fraudulent activity, FINRA reminds its membership in Notice 21-18 that there are numerous fundamental industry rules that require member firms to gather, retain and safeguard customer information. For the sake of brevity, we refrain from elaborating on the substance of each regulatory obligation and will merely mention the rules by name. A more robust description of these rules can be found within Regulatory Notice 21-18. In designing compliance programs to safeguard customer information, FINRA urges its membership to consider each of the following rules and regulations: FINRA Rule 2090 (Know Your Customer); SEC Regulation S-P, Rule 30; SEC Regulation S-ID; Customer Identification Program (CIP); FINRA Rule 4512 (Customer Account Information); FINRA Rule 3310 (Anti-Money Laundering Compliance Program); FINRA Rule 3110 (Supervision); Bank Secrecy Act; and Suspicious Activity Reports (SARs) with Fin Cen.

Best Practices Identified By FINRA

FINRA identifies the following as challenges common to all member firms:

- identifying effective methods of verifying the identities of customers who establish accounts online;
- 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);
- 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.

In order to combat against these challenges, FINRA offers the following best practices gathered from 20 different firms in the course of roundtable discussions.

A. Verifying a customer's identity at account opening

Similar to traditional methods of account opening, when onboarding customers online, member firms perform the following verifications themselves or through a third party vendor:

- validating identifying information or documents that applicants provide (*e.g.*, social security numbers (SSNs), addresses, and driver's license numbers), 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 (*g.*, automobile and home purchases).

B. Authenticating a customer's identity during login attempts

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. 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.

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); and

- the risk of the activity the customer wishes to perform (*g.*, checking an account balance or initiating a money transfer).

Risk thresholds 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.

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.

Many firms noted they transitioned away from using email addresses as authentication factors due to the prevalence of email breaches by bad actors.

C. Back-end monitoring and controls

Firms regularly conduct ongoing surveillance to detect and mitigate ATO threats. For example:

- monitoring at the customer account level for anomalies, such as:
  - significant amount of failed logins in a brief time period for a specific account; and
  - suspicious account activity (*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 all accounts for indications of credential stuffing or other large-scale attacks (*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);
- 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 (*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).

D. 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).

E. 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).

F. 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 (*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.

G. 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.

Additional Best Practices Based On Our Prior Experiences

In addition to the helpful best practices gathered by FINRA and outlined above, the attorneys at BCLP have significant experience in assisting firms with fraud matters and the design and implementation of new controls to help mitigate and safeguard against such activity. Below are some additional suggestions that we hope firms find helpful.

Customer Considerations:

1. **Passwords**. When customers establish online access, it is a good practice to require the use of a certain unique combination of letters (uppercase and lowercase), numbers and symbols to optimize fraud mitigation. Firms should consider requiring the passwords to be a combination of at least 8, 12 or even 16 characters in length. Firms should also consider requiring customers to update passwords periodically and block the use of prior passwords or iterations thereof. Customers should be encouraged to select combinations that do not incorporate readily available identifying information (such as their name, their children's name, SSNs, birthdates, etc.). Moreover, combinations with multiple uses of the same letter, number or symbols, or ascending or descending sequences, should not be permitted (i.e., 1, 1, 1, 1 or 1, 2, 3, 4).

2. **Notification related to change of e-mail addresses**. When a customer purportedly changes an e-mail address, firms should send notices to the prior and new e-mail address similar to what is often done for a traditional physical address change. This however, is often not enough to guard against fraud given the frequency of e-mail compromises. We would recommend that firms also consider sending some other form of notification to the account holder whether by hard copy mail to the mailing address used to establish the account or by SMS message or something similar.

3. **E-mailed instructions to transfer money**. This is a common fraud tactic that takes place in the securities industry. A fraudster will compromise a customer's e-mail address and send instructions to the firm to transfer money from the customer's brokerage account to an account elsewhere under the fraudster's control. These e-mails often include some degree of urgency and an indication that the account holder does not have the time or ability to discuss the instructions. In order to guard against this fraud, firms should not accept client instructions through e-mail communications but should rather consider requiring a signed letter of authorization from a client in order to transfer funds. By requiring such, the firm can verify the client's identity through a signature verification. In addition, before any transfer is carried out, someone from the firm should initiate a telephone call with the customer to first verify the customer's identity and then verify the instruction. A best practice would be to document the telephone call by noting what identifying information was requested and the customer's response to each question. Some firms go even further by requiring a similar second telephone verification call with the customer through the firm's wire desk.

4. **E-mail surveillance**. It would be a good practice for firms to monitor for multiple unrelated accounts linked to the same e-mail address as such activity might be indicia of fraud.

5. **Transfers of money away from the firm, particularly to third parties**. Anytime a customer transfers money away from the firm, the firm should consider initiating a telephone call to the customer. Such a call should have two purposes – verifying the identity of the customer as well as the validity of the transfer instructions. This is particularly true in instances in which the money is transferring to a third party or an account with a name that is not identical to the account holder.

6. **Annuity liquidations and withdrawals**. Annuities are often a target of fraud given that the assets are held at an annuity carrier rather than with the actual brokerage firm. Accordingly, member firms should consider requiring that all full and partial liquidations are supervised through a telephone call to the customer. Consistent with the call described above, a call to the customer should have two purposes – verifying the identity of the customer as well as the validity of the liquidation instructions.

Financial Advisor Considerations:

1. **Passwords**: The same password considerations for clients, as discussed above, would be applicable to financial advisors logging into their workstation.

2. **Prohibition on possessing client passwords**. Financial advisors should never be in possession or control of a customer's password(s) to any online account (internal or external). Similarly, financial advisors should not be permitted to help set up a customer's online access; rather, the firm should provide a separate hotline independent of the financial advisor to assist clients with such activity.

3. **Controls for computer station**. Financial advisers should be required to lock their computer stations if they are not in direct eyesight of those devices. Moreover, financial advisors should be prohibited from using laptops in public and all computer devices should be equipped with time-out software designed to automatically lock computers that have not been in use for a certain time period.

4. **Controls for client files**. All customer information should be locked when stored and never accessible to unauthorized users. No customer files should be removed from firm offices and electronic data should never be removed from firm devices.

5. **Outgoing Transfers**. Firms should consider monitoring all funds transferred outside the firm for any distributions to a financial advisor, or a creditor or institution F/B/O a financial advisor, directed out of an account not belonging to the financial advisor.

6. **Fraud Hotline**. Firms should consider providing customers with a hotline for contacting the firm independent of the financial advisor and his/her branch. Similarly, all branch personnel should be educated on the firm's procedures for reporting fraudulent activity.

Conclusion

With innovation comes an increase in cyber fraud. Firms must remain vigilant regarding new fraudster tactics and remain focused on safeguarding customer accounts by monitoring and detecting fraudulent activity. While FINRA outlined some helpful best practices in its Regulatory Notice 21-18, and we add some additional thoughts within this alert, this topic is forever evolving and requires ongoing effort on the part of member firms and the industry as a whole. By member firms sharing ideas and experiences, we, as an industry, can work together more efficiently and effectively to eradicate fraudulent activity, in all of its many and evolving forms.

If you have questions on this topic or need assistance with securities regulatory or litigation matters, including those involving fraud, please reach out to us as we would be delighted to help with your legal needs.

RELATED PRACTICE AREAS

- Broker-Dealer and Investment Advisor Regulatory Enforcement, Disputes and Investigations
- Financial Regulation Compliance & Investigations

MEET THE TEAM

Shea O. Hicks

St. Louis

shea.hicks@bclplaw.com
+1 314 259 2659

Eric Martin

St. Louis / Los Angeles

eric.martin@bclplaw.com
+1 314 259 2324
