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.[1]

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")[2] 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).[3] 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
FINRA Rule 2090 (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."[4] 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).[5] 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.[6] The CIPs must also describe when they will use documentary, non-documentary or a combination of both methods for identity verification.[7]

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)[8] with FinCEN.[9]

Common Challenges to Protecting Customer Accounts

During the roundtable discussions with FINRA, firms discussed the following cybersecurity challenges[10] they have encountered when safeguarding customer accounts from ATOs:

- identifying effective methods of verifying the identities of customers who establish accounts online;[11]
- 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).[12]

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.[13] 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);[14]
- 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 Compliant 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.[15]

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

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*:

Biometrics – the unique physical identifiers (*e.g.,* fingerprint, voice and facial recognition) or behavioral characteristics (*e.g.,* mouse activity and keyboard strokes on computers; touchscreen behavior and device movement on mobile devices) humans display to digitally authenticate their identity.
Credential Stuffing – 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.
Dark Web – the portion of the Internet that can only be accessed through special types of software and is often used to anonymously conduct illegal activity.
Impossible Travel – 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 (*e.g.*, logging in from Cleveland, Ohio and then, twenty minutes later, from Salt Lake City, Utah).
Likeness Check – 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).
Media Access Control (MAC) – a unique identifier used to identify a specific hardware device at the network level.
Penalty Box – a tool that isolates Internet Protocol (IP) addresses that exhibit potentially malicious behavior.
Planted Account – 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.
Short Message Service (SMS) – a system for sending short messages (*e.g.,* text) over a wireless network.
Trusted Device – 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".
Web Application Firewall (WAF) – 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.