Published on *The National Law Review* https://natlawreview.com

FINRA Shares Practices Firms Use to Protect Customers from Online Account Takeover Attempts and Opens Dispute Resolution Services

Article By:

Susan Light

Shelby Kost

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

On April 11, the Financial Industry Regulatory Authority (FINRA) issued Regulatory Notice 21-18 (Notice) in response to increasing reports from customers experiencing customer account takeover (ATO) incidents. These incidents involve bad actors using compromised customer information, including login credentials, to gain unauthorized entry to customers' brokerage accounts. FINRA reported the increase in ATOs comes as more firms offer online accounts.

FINRA published the Notice to remind members of their regulatory obligations to protect customer information. The Notice also summarizes the findings of roundtable discussions FINRA organized with member firms to identify best practices to mitigate risks associated with ATO attacks.

The existing regulatory obligations FINRA highlighted include FINRA Rule 2090, which requires firms to use "reasonable diligence" when opening and maintaining each account and to know the "essential facts" about each customer. Additionally, SEC Regulation S-P, Rule 30, requires firms to have written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer records and information that are reasonably designed to keep customer records and information secure and confidential. These policies must also protect against anticipated threats or hazards to customer records and information, including unauthorized access by bad actors. SEC Regulation S-ID requires firms to develop and implement a written program designed to detect, prevent and mitigate identity theft. In designing these programs, firms should consider, among other things, the methods of accessing covered accounts and detecting red flags of identity theft. Finally, pursuant to FINRA Rule 3310(b), firms' anti-money laundering compliance programs must establish, document and maintain written Customer Identification Programs (CIPs). These CIPs must include, among other things, risk-based procedures that enable firms to form a reasonable belief that they know the actual identity of each person opening a new account.

The Notice discussed key practices identified at the roundtable discussions that firms adopted to

mitigate ATO-related risks. For example, firms that onboard customers online can verify potential customers' identities by validating identifying information or documents, including Social Security numbers, addresses and driver's licenses, asking follow-up questions, or requesting additional documents to validate their identities. Firms can also require its customers to use multifactor authentication (MFA), which significantly reduces the likelihood that bad actors can gain access to a customer's account. The Notice also discussed various back-end monitoring and controls firms can implement, including monitoring at the customer account level for anomalies such as increases in the number of failed login attempts, monitoring emails received from customers for red flags of social engineering such as grammar issues, unexpected attachments or links, and establishing back-end controls to prevent bad actors from removing money from customer accounts, such as requiring a phone call with the customer on an established phone number.

FINRA Regulatory Notice 21-18.

FINRA Dispute Resolution Services to Reopen Most Hearing Locations for In-Person Arbitration and Mediation

Beginning on June 5, the Financial Industry Regulatory Authority Dispute Resolution Services (FINRA DRS) will permit in-person hearings to resume at most of its hearing locations for in-person arbitration and mediation proceedings. In-person hearings scheduled for Augusta, Boca Raton, Buffalo, Detroit, Philadelphia, Providence and Wilmington are postponed through July 30 and all affected parties will be contacted by FINRA DRS to discuss virtual hearing options or to reschedule in-person hearings.

FINRA DRS also detailed safety protocols to be implemented at each in-person hearing venue. For example, hearings will be held in venues large enough to allow for social distancing and cleaning, and sanitizing stations will be located in each room. Masks will be required for all participants. Plexiglas dividers or face shields will also be provided in the event testifying witnesses need to remove their masks. Participants will be required to complete a written health questionnaire.

FINRA DRS will continue to monitor the public health conditions in each of its 69 hearing locations. FINRA DRS Reopening Announcement.

National Law Review, Volumess XI, Number 134