Regulatory Notice 23-06

Heightened Threat of Fraud

FINRA Shares Effective Practices to Address Risks of Fraudulent Transfers of Accounts Through ACATS

March 28, 2023

Notice Type
- Guidance

Suggested Routing
- Anti-Money Laundering
- Compliance
- Cybersecurity
- Financial Crimes
- Fraud
- Information Technology
- Internal Audit
- Legal
- Operations
- Risk
- Senior Management
- Trading

Key Topics
- ACATS
- Asset Transfers
- Customer Nonpublic Information
- Cybersecurity
- Financial Crime
- Fraud
- Internal Controls
- New Accounts

Referenced Rules & Notices
- Regulation S-ID
- Regulation S-P
- Regulatory Notice 20-13
- Regulatory Notice 21-18
- Regulatory Notice 22-18
- Regulatory Notice 22-21

Summary

To bring attention to a rising trend in the fraudulent transfer of customer accounts through the Automated Customer Account Transfer Service (ACATS), FINRA issued *Regulatory Notice* 22-21, which alerted member firms about how bad actors effect fraudulent transfers of customer assets using ACATS (referred to as ACATS fraud). That *Notice* listed several existing regulatory obligations that may apply in connection with ACATS fraud and provided contact information for reporting the fraud.

FINRA's regulatory programs—through examinations and investigations, review of customer complaints and member firm engagement—have identified increased instances of ACATS fraud. Through recent industry engagement, FINRA has gained further insights from member firms and other industry representatives about their approaches to detect and mitigate the risk of ACATS fraud. This *Notice* provides an overview of some indicators of ACATS fraud and the practices some firms apply to address it.

This *Notice* does not create new legal or regulatory requirements or new interpretations of existing requirements, nor does it relieve firms of any existing obligations under federal securities laws and regulations. Member firms may consider the information in this *Notice* in developing new, or modifying existing, practices that are reasonably designed to achieve compliance with relevant regulatory obligations.

Questions regarding this *Notice* should be directed to AskAML@finra.org.

Background and Discussion

ACATS is an automated system that facilitates the transfer of customer account assets from one firm to another. National Securities Clearing Corporation (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.[1] In addition, the rule states that the carrying member must complete the transfer within three business days following the validation of the TIF.[2]

A bad actor, however, may use the efficiencies ACATS offers to effect the fraudulent transfer of customer account assets—ACATS fraud—by opening a new brokerage account online or through a mobile application at another firm (receiving member) using stolen personal identifiable information of a legitimate customer of another member firm. The bad actor may then engage receiving and/or carrying members to conduct a transfer of the account of the legitimate customer at the carrying member into the new brokerage account at the receiving member. When that transfer is complete, the bad actor may then proceed with moving the ill-gotten assets out of the newly established brokerage account to another external account or financial institution.

Potential Indicators of ACATS Fraud

Listed below are potential indicators of ACATS fraud that FINRA has observed through its regulatory programs:

- **Repeated Rejections of TIFs (Transfer Requests)** – Due to incomplete or inaccurate information, such as errors in account type or other basic account information, carrying member's rejection of receiving member's account transfer request for the same customer on multiple occasions.[3]
- **Request for Asset Transfer Soon After New Account is Opened** – Soon after the assets have been moved into a new brokerage account, a bad actor sends instructions to quickly move the assets to another external account or financial institution.
- **Changes in Customer Communication** – Changes in a customer's communication patterns, such as:
  - a customer who usually communicates with the firm by telephone instead of email now prefers to communicate with the firm via email only, and when the firm contacts the customer through the customer's usual means of communication (*e.g.,* telephone), the customer confirms that the email communication did not come from the customer; or

- a customer who has a long-standing relationship with the firm, requests to transfer assets to a receiving member via an email communication, which contains significant grammatical and spelling errors, or reflects a writing style that differs from previous email communications.

Other general indicators of new account fraud may also be a preliminary indicator of potential ACATS fraud.

Practices to Mitigate Risk of ACATS Fraud

As part of our member firm engagement, firms have shared some practices they have implemented to mitigate the risk of ACATS fraud. Some of these practices are consistent with those described in *Regulatory Notices* 21-18 and 20-13, and the 2023 Report on FINRA's Examination and Risk Monitoring Program. The practices include:

- **Verifying Customer Identities for Accounts Established Online** – Receiving and carrying members have indicated that they have implemented a variety of protocols to verify the identity of a customer that include:
  - a supervisory system reasonably designed, with principal review and approval, to address risks relating to automated approval of multiple accounts opened by a single customer in a short period (*e.g.,* same day or rapid online opening of accounts under the same name);
  - validating identifying information or documents using technology (*e.g.,* "likeness checks"[4]) and asking follow-up questions, or requesting additional documents based on information from credit bureaus, credit reporting agencies or digital identity intelligence (*e.g.,* automobile and home purchases);
  - contracting with third-party vendors to provide additional support with the customer account verification process (*e.g.,* databases to help verify the legitimacy of suspicious information in customers' applications);
  - requiring both primary (*e.g.,* original driver's license) and supplementary (*e.g.,* financial statement) documentation to verify client identity;
  - reviewing account application fields—such as telephone number, address, email address, bank routing numbers and account numbers—for repetition or commonalities among multiple applications that use different customer names or identifiers;
  - using technology to detect indicators of automated scripted attacks in the digital account application process (*e.g.,* extremely rapid completion of account applications from the same device or internet protocol (IP) address); and
  - using micro-deposits to verify customers in conjunction with other verification methods.[5]

- **Verifying Transfer Requests** – Receiving member confirms the accuracy and authenticity of an account transfer request, including:
  - reviewing for red flags of forgery and falsification in the digital signature the customer uses to complete the account transfer instructions, such as a signature that originated from an email address that was inconsistent with customer email addresses on file, or IP addresses or other data indicate a discrepancy between the location of the individual affixing the customer's digital signature and the customer's known residence;[6]
  - engaging third-party vendors to detect inconsistencies in customer profile information (*e.g.,* the search conducted by the third-party vendor returns a different name than the customer name provided for the Social Security number);
  - reviewing the number of times the carrying member has rejected a request, verifying customer account information for account transfer requests rejected by the carrying member due to incomplete or inaccurate information, and documenting the underlying reasons for rejection (*e.g.,* account title does not match the carrying member's records, incorrect account type); and
  - obtaining a copy of the customer's most recent statement for the account slated for transfer.
- **Enhancing Review of a Transfer Request** – Carrying member conducts additional review and verification on ACATS transfer requests, including:
  - notifying the customer through a mobile application push notification, email or phone call that an account transfer instruction has been received and directing the customer to promptly contact the member firm if the instruction was made in error or was not made by the customer;
  - identifying and addressing situations where an atypical number of accounts are moving in patterns to the same receiving member; and
  - engaging with the representatives assigned to the customers' account and operations staff assigned to handle the firm's account transfer process to confirm that the transfer was expected and provide training in risk mitigation practices.
- **Escalating to Anti-Money Laundering (AML)** – Carrying and receiving members adhering to SAR reporting requirements and escalating indicators of potentially fraudulent account transfers to the AML program, including red flags of identity theft detected during customer onboarding or the processing of account transfer requests (*e.g.,* rejections of account transfer requests related to the same customer and account transfer requests for the same customer from multiple broker-dealers).[7]

- **Investigating Fraud** – Carrying and receiving members thoroughly investigating potentially fraudulent account transfer requests and unsuccessful attempted fraudulent account transfer requests, including situations where member firms become aware of fraudulent account transfer requests after they are completed.

Reporting Fraud

FINRA urges member firms to evaluate their supervisory systems and compliance programs relating to transfers of customer assets using ACATS, including addressing risks of ACATS fraud. In addition to filing any required SARs through the BSA E-Filing system, FINRA also encourages its member firms to protect investors, the markets and other firms by immediately reporting[8] 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;
- for cybercrimes, 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.[9]

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

Endnotes

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. *See* generally Rule 11870(d)(3).
4. A "likeness check" is 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). *See Regulatory Notice* 21-18 (FINRA Shares Practices Firms Use to Protect Customers From Online Account Takeover Attempts).
5. *Regulatory Notice* 20-13 (FINRA Reminds Firms to Beware of Fraud During the COVID-19 Pandemic) noted that, while some firms use micro-deposits to verify customers, fraudsters may undermine this verification method, so the *Notice* advised that firms carefully watch for rapid withdrawals from accounts that were verified using micro-deposits and listed examples of how firms that used this method have confirmed customers' identities (*e.g.,* 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).
6. *See Regulatory Notice* 22-18 (FINRA Reminds Firms of Their Obligation to Supervise for Digital Signature Forgery and Falsification).
7. *See also Regulatory Notices* 20-13, 20-32 (FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection with Potential Account Takeovers and New Account Fraud), 21-14 (FINRA Alerts Firms to Recent Increase in ACH "Instant Funds" Abuse) and 21-18.
8. Firms should also consider whether ACATS fraud incidents may require firms to report the event pursuant to FINRA Rule 4530 (Reporting Requirements).
9. *See* www.nasaa.org/contact-your-regulator for the contact information for state securities regulators.