Regulatory Notice 22-21

Heightened Threat of Fraud

FINRA Alerts Firms to Recent Trend in Fraudulent Transfers of Accounts Through ACATS

October 6, 2022

Notice Type
- Special Alert

Suggested Routing
- Compliance
- Financial Crimes
- Fraud
- Internal Audit
- Legal
- Operations
- Risk
- Senior Management
- Trading

Key Topics
- ACATS
- Asset Transfers
- Fraud
- New Accounts

Referenced Rules & Notices
- Bank Secrecy Act
- FINRA Rule 2090
- FINRA Rule 3310
- FINRA Rule 4512
- FINRA Rule 4530
- FINRA Rule 11870
- NSCC Rule 50
- Regulatory Notice 20-13
- Regulatory Notice 20-32
- Regulatory Notice 21-14
- Regulatory Notice 21-18

Summary

FINRA alerts member firms to a rising trend in the fraudulent transfer of customer accounts through the Automated Customer Account Transfer Service (ACATS), an automated system administered by the National Securities Clearing Corporation (NSCC), that facilitates the transfer of customer account assets from one firm to another.

This *Notice* provides an overview of how bad actors effect fraudulent transfers of customer accounts using ACATS (referred to as ACATS fraud), lists several existing regulatory obligations that may apply in connection with ACATS fraud, and provides contact information for reporting the fraud. As FINRA continues to gather additional information related to ACATS fraud, FINRA is committed to providing guidance, updates and other information to help member firms stay informed about the latest developments, and will supplement this *Notice*, as appropriate.

Questions regarding this *Notice* should be directed to Jason Foye, Senior Director, Special Investigations Unit, at (561) 443-8062 or by email at Jason.Foye@finra.org.

Background & Discussion

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]

In general, a customer who wishes to transfer securities account assets from the carrying member to another firm must open an account at the new firm that is expecting to receive the customer's account assets (receiving member). The account transfer process begins when the receiving member receives the customer's authorized TIF; the receiving member then initiates the account transfer through ACATS.[3] Typically, a TIF includes the customer's name, date, the account type and account numbers at the receiving member and carrying member, and other personal identifiable information about the customer (*e.g.,* tax identification number or Social Security number).[4]

Overview of ACATS Fraud

In a situation where customer account information is stolen, a bad actor may use this information to effect ACATS fraud. In general, ACATS fraud may unfold in the following manner:

Using the stolen identity of a legitimate customer of a carrying member, a bad actor will open a brokerage account online or through a mobile application in the name of the legitimate customer at the receiving member to create a new account. The bad actor may open the new account solely using stolen information or with a combination of stolen and false information (*e.g.,* false email address or phone number).

Shortly after successfully opening the new account at the receiving member—generally, within a few days or weeks—the bad actor will then provide the receiving member with a TIF to initiate a transfer through ACATS of the legitimate customer's account assets from the carrying member.

Once the ACATS transfer of the assets to the newly established account at the receiving member is completed, the bad actor will (within a short period of time) attempt to move the ill-gotten assets to an external account at another financial institution by:

- transferring the account assets (*i.e.,* cash and securities) to an account at another financial institution;
- liquidating the securities or a portion of the securities transferred into the new account, then transferring any realized proceeds (along with any cash that was transferred to the new account) to an account at another financial institution; or
- purchasing additional securities using the transferred cash and then transferring those securities to an account at another financial institution.

ACATS fraud is related to the growing threat of new accounts being opened online or through mobile applications using stolen or synthetic identities.[5] In connection with the COVID-19 pandemic, FINRA previously advised member firms that bad actors may be "targeting firms offering online account opening services and perhaps especially, firms that recently started offering such services" by using stolen or synthetic identities to establish new accounts at member firms as a way to "divert congressional stimulus funds, unemployment payments or to engage in automated clearing house (ACH) fraud."[6] Similarly, with ACATS fraud, bad actors may be taking advantage of the efficiencies of the account transfer process offered through ACATS to fraudulently transfer assets out of an existing account of a legitimate customer whose identity is stolen to a new account the bad actor established at another broker-dealer using the stolen identity.

Relevant Regulatory Obligations

FINRA reminds its member firms of existing regulatory obligations that may apply in connection with ACATS fraud, including:

- FINRA Rules 2090 (Know Your Customer) and 4512 (Customer Account Information);
- the requirements of the Bank Secrecy Act and its implementing regulations and FINRA Rule 3310 (Anti-Money Laundering Compliance Program), including the requirements to maintain customer identification programs to verify the identity of each customer,[7] establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of Suspicious Activity Reports (SARs) with U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN),[8] and to conduct ongoing customer due diligence, including monitoring to identify and report suspicious transactions;[9]
- the Identity Theft Red Flags Rule (Regulation S-ID); and
- the processing of customer account transfers through ACATS in compliance with FINRA Rule 11870 (Customer Account Transfer Contracts).

Reporting Fraud

In addition to filing any required SARs through the BSA E-Filing system, FINRA also encourages firms to immediately report 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;
- 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.[10]

In situations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, broker-dealers should immediately notify by telephone an appropriate law enforcement authority.[11]

Endnote

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. Some transfers may occur outside of ACATS. *See* Rule 11870(a)(2). This *Notice* focuses on the transfers that occur within ACATS.
4. *See, e.g.,* FINRA Rule 11870.03 (Sample Transfer Instruction Form). *See also* DTCC ACATS User Guide (August 2, 2022) (ACATS User Guide) (listing the information the ACATS system sources from the TIF that includes receiving and deliverer (*i.e.,* carrying) broker-dealer; customer name; customer account number; Social Security numbers, among other data).
5. A synthetic identity may include legitimate Social Security numbers with false names, addresses and dates of birth. Without a clearly identifiable victim, a synthetic identity may go undetected for longer periods of time.
6. *See* Regulatory Notice 20-13 (May 2020) (reminding firms to be aware of fraud during the pandemic). *See also* Regulatory Notices 20-32 (September 2020) (reminding firms to be aware of fraudulent options trading in connection with potential account takeovers and new account fraud); Regulatory Notice 21-14 (March 2021) (alerting firms to recent increase in ACH "Instant Funds" abuse); and Regulatory Notice 21-18 (May 2021) (sharing practices firms use to protect customers from online account takeover attempts).
7. *See* FINRA Rule 3310(b) and 31 C.F.R. § 1023.220.
8. *See* FINRA Rule 3310(a) and 31 C.F.R. § 1023.320.
9. *See* FINRA Rule 3310(f) and 31 C.F.R. § 1023.210(a)(5).
10. *See* NASAA, Contact Your Regulator (providing contact information for state securities and provincial securities regulators and other resources those agencies provide).
11. Firms may call FinCEN's Hotline at (866) 556-3974.