Regulatory Notice 20-32

Options Trading

FINRA Reminds Firms to Be Aware of Fraudulent Options Trading in Connection With Potential Account Takeovers and New Account Fraud

September 17, 2020

Notice Type
- Reminder

Suggested Routing
- Anti-Money Laundering
- Compliance
- Fraud
- Internal Audit
- Legal
- Operations
- Options
- Systems
- Technology

Key Topic(s)
- Account Takeover
- Cyber Crime
- Identity Theft
- New Account Fraud
- Options

Referenced Rules & Notices
- Regulatory Notice 20-13

Summary

FINRA has recently observed an increase in fraudulent options trading being facilitated by (1) account takeover schemes (sometimes referred to as account intrusions), through which a bad actor gains unauthorized entry to a customer's brokerage account; and (2) the use of new account fraud[1] by a bad actor who fraudulently establishes a brokerage account through identity theft.

This *Notice* provides member firms and associated persons with information regarding options transactions in connection with these account takeover and new account fraud schemes to help identify, prevent and respond to such activity.

Questions regarding this *Notice* should be directed to:

- Danny Mileto, Vice President, FINRA Market Regulation, at (212) 457-5323 or *Danny.Mileto@finra.org*; or
- Kathryn Moore, Associate General Counsel, FINRA Office of General Counsel, at (202) 728-8200 or *Kathryn.Moore@finra.org*.

Background and Discussion

Overview

FINRA has recently observed an increase in fraudulent options trading being facilitated by account takeover schemes and new account fraud. An account takeover scheme commonly involves a bad actor improperly accessing a customer's brokerage account to purchase or sell securities at inferior prices. The bad actor may access a customer's brokerage account using compromised customer information or records, such as login credentials of a customer. New account fraud is a similar scheme and involves a bad actor establishing a brokerage account without the victim's knowledge through identity theft (often with funds stolen from the identity-theft victim's bank account) or

through a synthetic identity.[2] At the same time as the account takeover or the opening of the fraudulent new account, the bad actor uses a separate account at another broker-dealer to trade against these accounts in order to profit in this separate account.

Fraudulent Options Trading

While the risks associated with account takeovers and new account fraud are not new, FINRA has recently observed an increase in the use of fraudulent options trading associated with these schemes. In particular, some factors associated with options trading are conducive to the scheme, such as the financial leverage inherent to options and the availability of multiple options series, some of which have less liquidity and wider quote spreads. For example, these scenarios generally may involve the following circumstances:

- out-of-the-money listed calls and puts that have low theoretical values and relatively minimal market interest, leading to less liquidity and wide bid-ask spreads;
- the bad actor (profiting account) purchases options at low prices, under a $1 premium (*i.e.,* $100 notional value), and sells them at considerably higher prices (double or triple the purchase price), sometimes on the same day or within days of the purchases; often the purchase occurs first, but the sale could precede the purchase;
- the account taken over or opened fraudulently (victim account under the control of the bad actor) purchases options at high prices from the profiting account; and
- the options executions—particularly the sales by the profiting account while within the wide bid-ask spreads—do not reflect true market valuations, and would not likely have occurred if not for the purchases by the victim account that was subject to the account takeover or new account fraud.

Considerations and Resources for Firms

The protection of customers' non-public information is a key responsibility and obligation of FINRA member firms. FINRA has published Notices and guidance to assist firms in addressing cybersecurity risks.[3] These resources include a checklist of steps a member firm should consider if it learns that an unauthorized person may have gained entry to a customer's brokerage account,[4] as well as other steps firms may take to enhance their security practices, such as implementing multi-factor authentication to supplement password logins.

FINRA also reminds firms to be vigilant regarding customer accounts that are established to profit from options trading facilitated by account takeover schemes and the use of new account fraud.[5] The customer accounts profiting from this type of conduct may be in the names of non-U.S. persons, with fund transfers through non-U.S. banks. However, accounts may also be in the names of U.S. individuals, particularly those who had their identities stolen. When potential activity related to the above noted schemes has been

identified, member firms should immediately commence reviews to determine whether action is appropriate, such as placing trading and fund restrictions on the relevant profiting accounts.

Account takeover schemes and new account fraud may trigger legal or regulatory obligations for firms housing either the victim or profiting accounts, such as filing a suspicious activity report (SAR) or, potentially, reporting to FINRA and relevant governmental authorities. Member firms should also proactively review their written supervisory procedures in light of the recent increase in the above noted schemes (*e.g.,* to consider whether they address the risk of compromised customer records and information).

Endnotes

1. *See* FINRA *Regulatory Notice 20-13* that discusses fraudulent account openings and money transfers.
2. A synthetic identity includes legitimate Social Security numbers (SSNs) with false names, addresses and dates of birth. Without a clearly identifiable victim, it may go undetected for longer periods of time.
3. These resources are available on FINRA's dedicated Cybersecurity and Customer Information Protection webpages.
4. *See* Firm Checklist for Compromised Accounts.
5. FINRA *Regulatory Notice 20-13* discusses fraudulent account openings and money transfers.