February 29, 2024

Threat Intelligence Product
Encrypted-Messaging Investment Club Scams

Financial Intelligence Unit

The **Financial Intelligence Unit (FIU)** within FINRA's National Cause and Financial Crimes Detections Program (NCFC) supports the protection of investors and markets by identifying and assessing threats and trends impacting the financial and securities industry and developing actionable intelligence for its stakeholders.

This TIP was prepared by FINRA's FIU and is based on internal data and intelligence and open-source information. Questions may be directed to **FIU@finra.org**.

This **TIP** 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, regulations and FINRA rules. Member firms may consider the information in this TIP in developing new, or modifying existing, policies and procedures that are reasonably designed to achieve compliance with relevant regulatory obligations based on the member firm's size and business model. Moreover, some questions may not be relevant due to certain firms' models, sizes or practices.

Threat Overview

This Threat Intelligence Product (TIP) provides an overview of FINRA's observations regarding a new threat involving fraudulent social media advertisements (ads) that direct readers to purported "investment clubs" on encrypted messaging applications, where victims are persuaded to purchase shares of low-volume and thinly traded securities listed on the U.S. and foreign exchange markets. The bad actors appear to be engaging in schemes in which they coordinate the victims' buying activity to drive up the price of a security, while shares of the same security are then liquidated by others. Since November 2023, FINRA has received numerous investor complaints alleging millions of dollars in losses.

The threat integrates aspects of other fraudulent schemes such as imposter and so-called "pig butchering" scams,[1] which are more widely associated with soliciting victims to invest in fraudulent cryptocurrency schemes, with minimal touchpoints to the securities markets. Recently, FINRA identified an increase in pig butchering schemes used to convince victims to purchase shares of U.S. small-capitalization exchange-listed issuers that recently held an initial public offering, as part of what is referred to as a "ramp-and-dump" scheme.[2]

These threats use the likeness of well-known investors and financial industry professionals, who are not affiliated with the scheme, to lure victims. The bad actors place banner ads on social media using the likenesses of these investors and professionals, impersonating them as part of their imposter scam. The ads claim the reader can invest alongside the well-known investors and promise high returns. Upon clicking the ad links, victims are routed to an "investment club" that is falsely advertised as being managed by employees of the impersonated investment professional. In many cases the "investment club" claims to be a registered investment adviser (RIA). The purported RIAs later direct victims to purchase shares of low-priced and low-volume securities listed on U.S. stock exchanges and, increasingly, on the Hong Kong stock exchange as part of the ramp-and-dump schemes.

FINRA's Investor Education Foundation published an article alerting the investing public that social media "investment group" imposter scams were on the rise.[3] FINRA has also shared intelligence regarding these scams with member firms, law enforcement and other regulators.

[1] *See* Cora Lewis, Investment scams are everywhere on social media. Here's how to spot one, Associated Press (August 17, 2023) and Adam McNeil, Trash Talk: Pig Butchering and Conversational Attacks Were the Fastest Growing Mobile Threats of 2022, Proofpoint (April 18, 2023).
[2] *See* FINRA Investor Insight This On-Ramp Could Lead You to a Dump (March 30, 2023) and FINRA *Regulatory Notice* 22-25 (Heightened Threat of Fraud).
[3] *See* FINRA Investor Insight Investor Alert: Social Media 'Investment Group' Imposter Scams on the Rise (January 11, 2024).

Background

FINRA has identified aspects of pig butchering and imposter scams as components of the social media "investment club" scheme.

- **Pig Butchering Scams** are a type of cyber-scam where bad actors attempt to build victims' trust before manipulating them into phony investments and disappearing with the funds. Bad actors contact individuals, often via a seemingly misdirected text message, and attempt to build rapport, often friendly or romantic. Over the course of days, weeks or even months of communication, bad actors solicit these individuals to invest money into fraudulent cryptocurrency or investment schemes.[4] Most recently, FINRA has observed the use of pig butchering scams to solicit investors to purchase shares of publicly traded companies that are the subject of market manipulation schemes.[5]

- **Imposter Scams** come in many varieties, but routinely involve a scammer pretending to be an experienced financial professional to convince victims to send money to the bad actors.[6] Typically, bad actors, using imposter websites and imposter social media personas, entice investors to invest money with these scammers through, among other tactics, testimonials describing positive returns.

Summary of the Investment Club Scam

A review of investor complaints, regulatory tips and FINRA investigations revealed the following information about the "investment club" scams:

- The bad actors publish ads on social media (primarily Facebook and Instagram) that use the likenesses of well-known investors to invite victims to join an investment club managed by the professional. Below are examples of ads on Facebook:

- Oftentimes, bad actors promise investors dazzling returns, well-researched stock picks and a community of like-minded individuals. Upon clicking an ad link, victims are taken to an "investment club"

[4] *See* Amanda Hetler, Pig butchering scam explained: Everything you need to know, TechTarget (February 28, 2023) and Poppy McPherson and Tom Wilson, Crypto scam: Inside the billion-dollar 'pig-butchering' industry, Reuters (November 23, 2023).
[5] *See* FINRA Investor Insight Pig Butchering' Scams: What They Are and How to Avoid Them (December 13, 2022)
[6] FINRA has similarly observed fraudsters establishing websites that impersonate FINRA registered representatives as a part of a cryptocurrency scam. *See* FINRA *Regulatory Notice* 20-30 (Fraudsters Using Registered Representatives Names to Establish Imposter Websites).

(often in WhatsApp, an end-to-end encrypted messaging application). The participants in the group chat appear to be a combination of bad actors, bots and numerous potential victims.

- Once in the encrypted messaging application, bad actors continue to impersonate well-known investors, utilize fictitious personas claiming to be RIAs, or impersonate legitimate RIAs or associated individuals.

- Within the group chat, bad actors recommend victims use their personal brokerage accounts, or open new accounts at member firms that provide access to trade on foreign markets, and trade in accordance with the bad actors' recommendations.

- The bad actors initially recommend victims invest in well-known blue-chip securities to gain the victims' trust. Then, the bad actors begin to recommend victims trade in low-priced/low-volume U.S.- or Hong Kong-listed stock. The bad actors advise victims on how to purchase the stock, including the type of order (usually one or more buy limit orders), when to place the order, how many shares the victim should purchase, and the price at which the victim should place the order. The bad actors request victims to send screenshots of their brokerage account holdings, and the limit orders placed, to the bad actors.

- The victims' purchasing activity occurs in conjunction with—and likely causes—price increases in the targeted securities. The bad actors instruct the victims to not sell the securities and may threaten victims with expulsion from the "investment club" if the victim does not follow the bad actors' instructions. The purchasing activity by the victims often coincides with liquidations of shares by accounts presumed to be controlled by the bad actors.

- Social media searches have revealed that in some instances the purchasing activity by the victims in some securities coincide with what appears to be bots posting information on X (formerly Twitter) hyping those securities.[7]

- The bad actors encourage victims to move all their available funds from other accounts into the existing or newly opened brokerage accounts. After victims report losses, the bad actors encourage victims to transfer more funds into the account, promising that the victims will make up their losses through additional investment. FINRA has observed bad actors trying to convince victims to borrow money from family and friends to continue their participation in these schemes.

[7] Social media searches have also uncovered social-media groups on Reddit.com and Facebook dedicated to the victims of these "investment club" scams.

Information on Bad Actors

FINRA has not been able to identify the true identities of the bad actors behind these scams due to, among other things, jurisdictional limits. Through FIU assessment of the bad actors orchestrating these scams, it is believed that the bad actors are most likely located overseas. This assessment is based on first-hand accounts of victims and open-source literature on pig butchering scams.

Best Practices to Identify and Mitigate Threat

FINRA encourages members to consider the following red flags and mitigation strategies to identify and mitigate "investment club" scams:

- Review correspondence with customers, or in customer complaints, for indication that an investor is being directed by an unknown or unfamiliar third-party.
- An investor is liquidating moderate or conservative investments to purchase one low-priced and low-volume U.S. exchange listed security, or a similar type of security listed on a foreign exchange.
- A sudden interest by multiple investors in a low-priced and low-volume U.S. or foreign exchange listed security, which could be observed through multiple buy limit orders being placed by investors at aggressive (*e.g.*, at or near the listed ask price) or increasing prices.
    - For these securities, conduct an internet search for allegations of the securities being used in fraudulent schemes.

Conclusion

This TIP provides an overview of FINRA's observations regarding a new evolution of imposter scams, pig butchering scams and ramp-and-dump schemes, impacting the U.S. and Hong Kong securities markets through the use of fraudulent social media ads and encrypted-messaging applications purporting to be "investment clubs."

FINRA encourages member firms that identify any occurrence of the above-described scam to report it to:

- FINRA using the Regulatory Tip Form found on FINRA.org;
- SEC's tips, complaints, and referral system (TCRs) or by phone at (202) 551-4790; and
- the FBI's tip line at 1-800-CALLFBI (1-800-225-5324) or at Internet Crime Complaint Center (IC3).