Suggested Routing: *Anti-Money Laundering, Compliance, Cyber, Financial Crimes, Fraud, Information Technology, Operations, Risk and Senior Management.*

This Threat Intelligence Product (TIP) is the first in a series of publications assessing adversarial use of generative artificial intelligence that results in harm to investors, broker-dealers and the securities market.

Bad actors are increasingly utilizing generative artificial intelligence (Gen AI) to produce high-quality, fraudulent media to trick victims into participating in "investment club" scams. This Threat Intelligence Product (TIP) provides details on this type of scam, as well as effective practices to recognize and mitigate this type of threat being enhanced by Gen-AI.

Threat Overview

This TIP focuses on protecting investors from bad actors' use of generative artificial intelligence (Gen AI)[1] in "investment club" scams, a scam in which bad actors use fraudulent social media advertisements to direct investors to purported investment clubs hosted on end-to-end encrypted messaging applications (such as WhatsApp and other platforms). The bad actors then persuade victims to purchase shares of low-volume and thinly traded securities listed on U.S. and foreign exchange markets, coordinating the victims' buying activity to drive up the price of a security, at which point the bad actors liquidate their own shares. Since November 2023, FINRA has received investor complaints alleging multiple millions of dollars in losses due to investment club scams. In February 2024, FINRA disseminated the Encrypted-Messaging Investment Club Scams TIP[2] that detailed these scams.

Gen AI–Enhanced Investment Club Scams

Advances in artificial intelligence, especially Gen AI, including large language models (LLMs) and generative adversarial networks (GANs),[3] allow bad actors to produce high-quality synthetic media,[4] such as deepfakes,[5] with limited to no technical experience. Moreover, the tools to create deepfakes are more widely accessible than ever before. FINRA has recently identified bad actors incorporating Gen AI–created synthetic media, such as text, images and videos, into these investment club scams. Listed below are some of the observed methods in which bad actors have exploited Gen AI to enhance these scams.

Deepfake Images and Videos

These scams typically begin with fake social media ads featuring well-known finance personalities—such as Bill Ackman, Jim Cramer or Cathie Wood—promoting a social media–based investment club. In the past, bad actors used publicly available images and videos to trick investors into thinking a famous person was behind an investment club, as shown in Figure 1. Now, bad actors are using Gen AI–created media, such as the video shown in Figure 2, to bolster their authenticity and credibility.

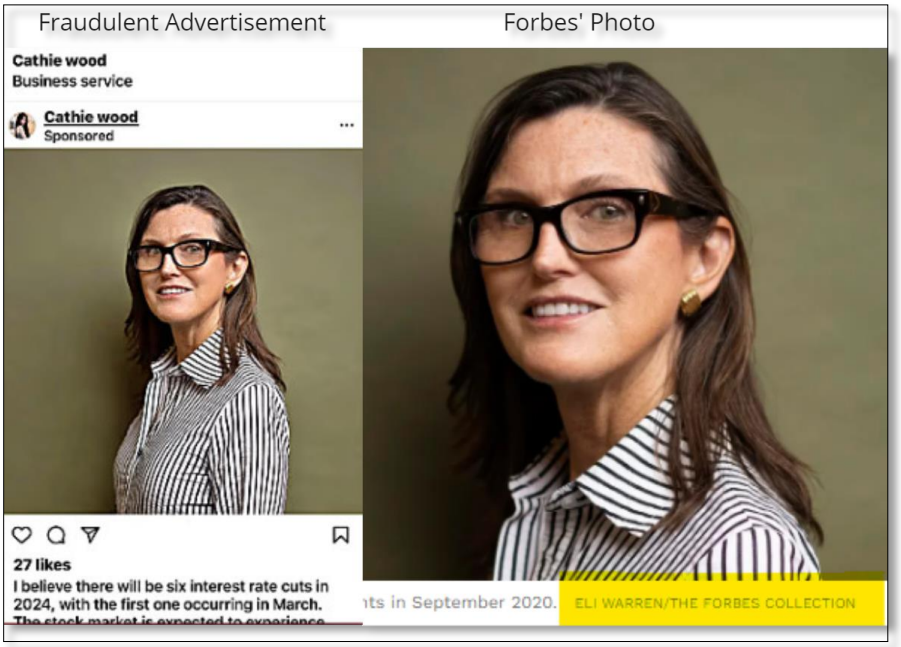

Figure 1: Fraudulent ad featuring a real photo of Cathie Wood.

Figure 2: Still image of Cathie Wood from a deepfake video used to promote a crypto scam.

As Gen AI has grown in popularity, a range of applications have been developed—including open-source and free tools—that can produce high-quality deepfakes of celebrities. Bad actors can use publicly available media featuring any person (*e.g.*, images or videos on video-sharing and streaming platforms, or content hosted on social media websites) to train a Gen AI video model and create deepfakes of that person.

Deepfake Audio

Similar to the creation of deepfake videos, bad actors have a range of applications to create convincing deepfake audio, including some that use celebrity voices, mostly unauthorized. Some Gen AI tools clone audio, offer premade voices (see Figure 3) and utilize text-to-speech capabilities that bad actors can use at minimal cost. As with deepfake videos, these websites and mobile apps have trained Gen AI audio models on publicly available media, such as podcasts, webinars and audio extracted from videos. Bad actors can then use free tools to synchronize the deepfake video and deepfake audio to complete the production.

Figure 3: Screenshot of Jim Cramer from a website that uses celebrity voices, without authorization, to promote investment club scams.

Gen AI-Created Text

Bad actors can further exploit Gen AI to streamline the creation of text for these social media investment club scams, including the content for the social media ads, scripts for deepfake videos and dialogue for conversations with victims. Gen AI tools make the process simple, as they require minimal input from the bad actor. Gen AI text-based tools can craft a compelling sales pitch to be used in a deepfake video (see Figure 4), a description of the investment club and the sign-up page that brings the victims to the club's chat group (see Figure 5). A bad actor can request that the Gen AI tool create multiple variations of the same content for use in other investment club scams.

Figure 4: Screenshot of ChatGPT's response to a request for a sales script.

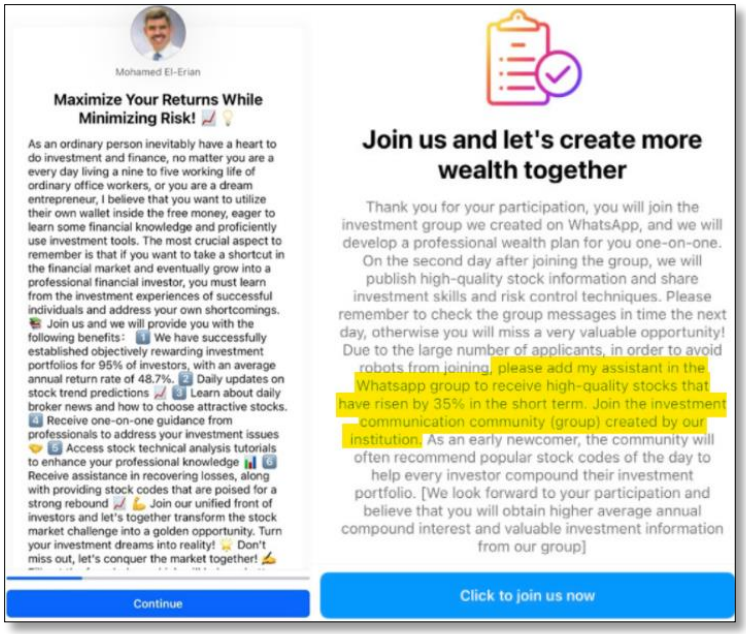

Figure 5: In-ad sign-up page for an investment club scam that uses, without authorization, a photo of Mohamed El-Erian.

Once a victim joins the encrypted messaging group, a bad actor posing as an "assistant" will contact the victim directly through the messaging app or via text message to gather information about the victim and provide investment instructions, as shown in Figure 6.

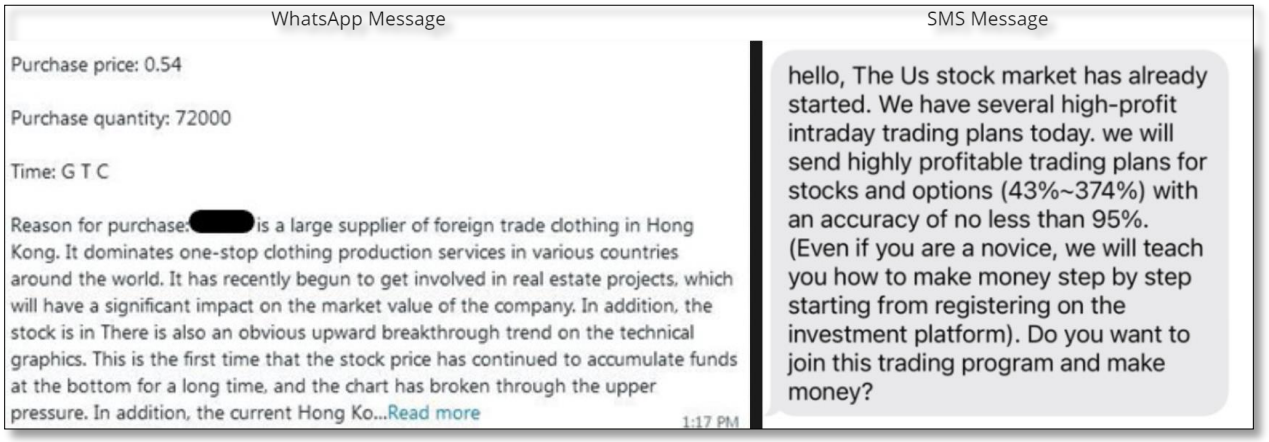

Figure 6: Communications by bad actors involved in fraudulent investment club scams.

Historically, these communications have often included informal language, poor grammar and effusive use of emojis. Other indications of red flags include terms like "US stock market" or "Us stock market"—rather than the more conventional "stock market"—that would alert potential victims that they might be dealing with non-native English speakers located abroad. In the future, Gen AI tools may help bad actors eliminate nearly all of these red flags.

Finally, the bad actor instructs the investors on how and when to purchase the target stock. The victimized investors' purchasing activity occurs in conjunction with, and contributes to, price increases in the targeted securities, which then coincide with the sale of shares by accounts presumed to be associated with bad actors. Bad actors may also be incorporating Gen AI, or will likely do so in the future, to make this specific process more effective (*e.g.*, using bots to post messages in investment club messaging apps that appear to be from other investors or to spread information on social media promoting the targeted securities).

Effective Practices to Identify and Mitigate the Threat

Member firms can help their customers mitigate the threat from Gen AI-enhanced fraudulent social media investment clubs and other related scams by learning how to identify synthetic media.

Member firms may consider encouraging their customers to:

- review FINRA's Investor Insights articles, Artificial Intelligence (AI) and Investment Fraud, and Social Media 'Investment Group' Imposter Scams on the Rise;
- conduct searches of the well-known finance personality appearing in an ad on a social media platform to confirm the legitimacy of the ad and whether that investor is publicly disclaiming his or her involvement in investment clubs;
- learn to identify visual and audio cues of deepfakes, such as blurred edges around the image of the purported well-known finance personality's face or body, discrepancies in skin tone around the hairline or ears, inconsistent hand sizes and number of fingers, out-of-place accessories like eyeglasses or earrings, out-of-sync lip movements, inconsistent pitch and voice inflections, and irregular pauses between words;
- compare publicly available video and audio of the well-known finance personality to that of the social media ad to determine whether the voice in the video and audio match;

- review the social media account of the individual posting the ad to determine if prior posts from that account seem suspicious (*e.g.*, other suspicious sales or marketing activity).
- be wary of glowing reviews of and comments on social media ads or in group messaging chats—especially where the reviews and comments appear to have been made in a short period of time—as the bad actors themselves may have created those statements;
- learn to identify red flags in text-based conversations, such as abrupt shifts between formal and informal language, misspellings of common industry terms and pushback when requesting the bad actor's location or the website of the investment club;
- conduct reverse image searches of photos of investment club administrators, assistants and secretaries, as those searches may surface stock photos or reveal the person to be someone other than who they say they are;
- adjust privacy settings for messaging apps to prevent being added to groups or private conversations by individuals not in one's contact list—oftentimes, once an individual joins an investment club group chat, he or she becomes a target and will receive invitations to join other investment club chats and/or private conversations where a bad actor will attempt other types of scams;
- leverage reputable software tools or browser plug-ins that can identify inconsistencies in metadata of videos, images and audio files that are potential indicators of manipulated or AI-generated content;
- report suspicious text messages from unknown individuals to cellphone providers and block the senders' phone numbers; and
- report suspicious ads to social media companies.

Conclusion

FINRA encourages member firms and their customers to report any instances of fraud to:

- FINRA using the Regulatory Tip Form found on FINRA.org;
- the SEC using the Tips, Complaints, and Referrals form or by calling (202) 551-4790; and
- the FBI using its Internet Crime Complaint Center or by calling 1-800-CALLFBI (1-800-225-5324).

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 disseminating actionable intelligence.

This TIP was prepared by FINRA's FIU. It is based on internal data 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 information may not be relevant due to certain firms' models, sizes or practices.

You received this email because you are designated as your firm's AML Compliance Contact, Chief Compliance Officer, Chief Information Security Officer, Chief Risk Officer, Regulatory Inquiries or Senior Investor Inquiries contact person in the FINRA Contact System (FCS). While the TIPs are not published publicly, we encourage you to forward this TIP on to others within your organization who may benefit and be able to assist in mitigating this threat. Please see suggested routing at the top of this message for potential applicable business areas.

---

[1] Gen AI is a type of artificial intelligence that, based on a user's prompt, can create content, such as text, computer code, audio, and video.

[2] FINRA's Investor Education Foundation accompanied the TIP with the Investor Insight Social Media 'Investment Group' Imposter Scams on the Rise.

[3] A "GAN" is a machine learning model that uses two neural networks to compete against each other to create new data that is similar to a given training dataset.

[4] Synthetic media is media that has been created or modified using artificial intelligence.

[5] Deepfakes, a type of synthetic media, are highly realistic multimedia, including text, images, sound, and videos, made using machine learning, a subset of artificial intelligence.