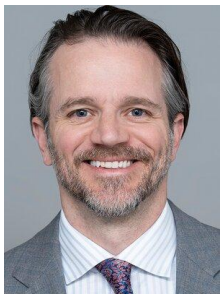
How The SEC Is Combating 'Investment Confidence Scams'

By **Kelly Lenahan-Pfahlert and Terence Grugan** (November 18, 2026)



Kelly Lenahan-Pfahlert



Terence Grugan

On Sept. 29, the U.S. Securities and Exchange Commission announced fraud charges against two clusters of entities alleged to have defrauded thousands of retail investors, including many in the U.S., out of at least $15.3 million through what the agency calls "investment confidence scams."[1]

In a pair of complaints filed in the U.S. District Court for the Southern District of New York, the SEC charged Cryptoaiml Ltd. and Cryptoaiml Capital Foundation with misappropriating more than $12.5 million from over 300 retail investors, and separately charged TSAI Pro Ltd. and TSAI Capital Foundation (also known as TSAI Exchange Ltd.) with stealing approximately $2.8 million from roughly 1,715 investors. Both sets of defendants are believed to be operated by unidentified individuals located overseas.

The two schemes shared a common architecture: the rapid creation of U.S. corporate entities, the filing of Forms D with the SEC containing fabricated information, registration as money services businesses with the Financial Crimes Enforcement Network, and the aggressive use of WhatsApp group chats and social media to recruit customers. The SEC has since removed the fraudulent Forms D from its website.

Together, the cases show an agency willing to look past sham paperwork and bring multiple legal theories against offshore schemes, even when the people behind them remain unidentified. They also expose how easily alleged bad actors can combine encrypted messaging, artificial intelligence buzzwords and fabricated regulatory credentials to manufacture an appearance of legitimacy and reach unsophisticated investors.

How the Alleged Fraud Worked

Cryptoaiml

The alleged Cryptoaiml scheme operated from approximately August 2024 through March 2025 and, according to the SEC's complaint, followed a carefully staged progression.

The defendants created a series of WhatsApp group chats with names like "VIP-Wealthy Affiliate Group," "Citadel AI Community" and "AI Advanced Community." In those chats, the defendants allegedly impersonated real, named investment professionals at well-known firms, including a purported representative of Raymond James & Associates and the actual president of Citadel Securities. None of these real professionals or their firms had any involvement.

The alleged impersonators claimed to share AI-generated trading signals with a purported 98% accuracy rate, directed investors to open accounts on a fake crypto trading platform, and posted fabricated testimonials from supposed satisfied investors to build confidence. The platform looked convincing, with real-time price displays and account dashboards showing growing balances, but no actual trading ever took place.

To bolster legitimacy, the defendants allegedly embedded on their website a screenshot of a Form D filed with the SEC and a money services business registration with FinCEN, both of which contained fabricated names, addresses and forged notarizations.

The endgame was blunt. When investors tried to withdraw their supposed profits, they were told their accounts were frozen and that they needed to pay advance fees to unlock them.

Payments were directed to U.S. bank accounts held by shell entities, including Flavyo Trading Corp., Neurotech IT Solutions Inc., INTY Endless LLC and a sole proprietorship called Enjoy Time. Investors were coached on what to tell their banks about the transfers.

Those funds were then allegedly wired to entities in the United Arab Emirates and to Chinese companies, commingled with funds of unknown origin. Some investors sold securities from brokerage accounts and 401(k)s to meet the defendants' demands.

TSAI

The TSAI defendants ran a parallel but distinct alleged scheme from September 2024 to March 2025, centered on a fake AI trading bot program. Investors were allegedly told they could earn guaranteed profits by depositing crypto-assets to rent AI-powered trading bots that would trade on their behalf. The bots ranged in price from $100 to $500,000; at the top end, the defendants promised returns of $17,500 per day for 360 days, according to the SEC.

The alleged scheme also incorporated a pyramid structure: Investors could earn commissions by recruiting others, with tiered levels from S0 to S7 and promises of monthly salaries and stock dividends for top recruiters.

As with Cryptoaiml, the entire operation was fiction, per the SEC. There were no AI trading bots, no real accounts and no actual trading. Like Cryptoaiml, the SEC claimed that TSAI also filed a Form D containing false information and posted a fabricated SEC certificate on its website to create the appearance of regulatory oversight.

When investors tried to withdraw funds, they were told their accounts were blocked for "suspicion of illegal arbitrage" or were required to pay fabricated taxes and verification payments. By March 2025, the website went dark entirely.

What It Means

The SEC brought overlapping but distinct claims in the two actions, and the legal theories are worth examining.

Both complaints allege violations of Section 10(b) of the Securities Exchange Act and SEC Rule 10b-5, targeting both the defendants' allegedly fraudulent misstatements and their broader deceptive schemes. But the two cases diverge in instructive ways.

The Cryptoaiml complaint additionally charges violations of Sections 206(1) and (2) of the Investment Advisers Act. The theory is that the defendants functioned as investment advisers because they allegedly entered into investment management agreements with at least two clients and held themselves out as providing securities advice for compensation.

This is a notable claim. According to the SEC, the advisory agreements were entirely sham

documents, one purporting to be from Cryptoaiml Venture Capital Management Group and another invoking the name of Raymond James & Associates. Yet the SEC is treating those purportedly sham agreements as sufficient to establish an advisory relationship and trigger the Advisers Act's fiduciary obligations.

That willingness to look through form to substance is significant, particularly in a space where fraudsters routinely adopt the language and trappings of legitimate financial services.

The TSAI complaint takes a different path. In addition to the standard anti-fraud charges and Securities Act Section 17(a) claims, the SEC charges violations of Sections 5(a) and 5(c) of the Securities Act for the sale of unregistered securities.

The premise is that the AI trading bot program allegedly constituted an investment contract under the framework developed in the U.S. Supreme Court's 1946 decision in SEC v. W.J. Howey Co.: Investors pooled their funds, were promised returns generated by the defendants' purported managerial efforts in developing and operating the trading bots, and could earn additional income through the pyramid recruitment structure.

This matters because the SEC did not need to prove that the bots actually existed or functioned to bring the Section 5 claim; the offering was the investment contract itself. It is another example of the agency's willingness to classify novel crypto-adjacent products as securities, and the registration charge gives the SEC an additional enforcement tool that does not require proof of scienter.

The Bigger Picture

These two actions are part of a broader pattern. Investment confidence scams that exploit encrypted messaging platforms and capitalize on public enthusiasm for AI are proliferating, and the SEC's willingness to bring multiple legal theories against offshore entities reflects the agency's determination to pursue these cases even when the individuals behind the schemes remain unidentified.

The cases also highlight a troubling feature of the current regulatory landscape: the ease with which alleged bad actors can file Forms D and register as money services businesses to manufacture an appearance of legitimacy.

The SEC has encouraged investors to use investor.gov to check the backgrounds of anyone offering or selling investments, and it has issued investor alerts specifically warning about fraudsters who use group chats or claim false SEC registration to lure victims. But as these complaints demonstrate, the purported fraudsters are getting more sophisticated in mimicking the markers of legitimate financial activity, and the combination of encrypted messaging, AI buzzwords and fabricated regulatory credentials is proving effective at reaching unsophisticated investors.

Kelly A. Lenahan-Pfahlert is a senior staff attorney at Ballard Spahr LLP.

Terence M. Grugan is a partner and co-leader of the anti-money laundering practice team at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective

affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] https://www.sec.gov/newsroom/press-releases/2026-95-sec-charges-multiple-entities-fraud-schemes-totaling-least-15-million-used-whatsapp-other-platforms.