Are You an Informed Investor?
Crypto Recovery Room Scams

November 2025

Getting calls, texts, messages or emails from someone promising to find or return money you lost in a crypto scam? Be careful, it's almost certainly a crypto recovery room scheme. Fraudsters are capitalizing on the increasing number of investors who have lost money to crypto investment scams by running recovery room schemes that aim to steal even more money from victims.

Crypto scams: A serious threat to North American investors

International criminal networks are actively targeting North American investors with sophisticated crypto schemes. U.S. and Canadian law enforcement agencies report that tens of thousands of crypto investment scams with losses in the multi-billions of dollars occur annually and are rising. The FBI reports that "cryptocurrency has become an enticing means to cheat investors, launder proceeds, and engage in other illicit activities."[1]

What is a crypto recovery room scam?

In a crypto recovery room scam, the fraudster mixes time-tested techniques with new digital technologies, including the blockchain, online communications platforms, websites and artificial intelligence (AI), to make the offer of recovering an investor's lost crypto for a fee seem legitimate. The fraudster's most dangerous weapon for stealing more money is using the investor's false hope of recovering their lost crypto. When the scammer touts their ability to recover lost crypto, they will demand that the victim use cryptocurrency like Bitcoin or Ethereum to pay the fake recovery fee which, like the original lost crypto, will be difficult to recover.

How a crypto recovery room scam works

Recovery scammers use multiple communication channels – direct messaging, phone calls, email, etc. – to contact victims they have already scammed. Once a scammer contacts their victim, the scammer will feign legitimacy by confirming the victim's crypto account or wallet, sometimes for a fee. They will offer to recover the victim's crypto for a fee, sometimes encouraging multiple payments that grow over time.

The fraudster may impersonate a law enforcement agency, a securities regulator, or an association (usually fake) that helps crypto fraud victims recover their funds. The scammers running these schemes are relentless

Continued

1 Federal Bureau of Investigation, Internet Crime Report 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. The CSA reports similar schemes occurring in Canada. See Canadian Securities Administrators, Canadians losing millions to investment scams: CSA, CAFC and RCMP urge vigilance and reporting (March 13, 2025), https://www.securities-administrators.ca/news/canadians-losing-millions-to-investment-scams-csa-cafc-and-rcmp-urge-vigilance-and-reporting/.

and aggressive. They will likely pressure the victim with frequent communications that may go on for weeks or months.

There are multiple ways scammers can obtain the contact information of people who've lost money in a fraud. They can buy or obtain contact lists of people who were scammed, look for investors who share their investment fraud stories online, or set up websites to lure victims looking to recover their crypto into contacting a fake asset recovery service.

How to identify crypto recovery room scams

- **Unsolicited communications –** If someone you don't know contacts you offering to recover money from a crypto scam you lost money to, it's almost certainly a recovery room scheme. Investment fraud is big business for international criminal gangs. Groups or individuals who run investment scams may have given your contact information to "a colleague" who is responsible for running the organization's recovery room. Your information may be sold on the Dark Web.

- **Use of new digital technologies and techniques –** Fraudsters use AI to develop communications – caller scripts, videos, audio recordings, etc. – to convince the victim that their offering is legitimate. For example, they can use AI to produce videos with testimonials from fake victims who then recommend the fraudster's services. They can customize these materials to appeal to victims in a variety of ways, including translating it to the victim's preferred language.

- **Fake recovery room websites –** An internet search on crypto asset recovery will reveal many websites offering to recover a victim's crypto. The websites often feature reviews and testimonials of successfully recovered funds. Creating these fake asset recovery websites and testimonials is an easy, low-cost way to ensnare vulnerable people.

- **Bait and switch –** Some scammers will make it look like they found an investor's crypto by creating fake coins that have a similar name or symbol of the lost asset. They will send the investor some of these fake crypto coins, which have no value, to make it look like they've recovered the asset. They offer to send the rest, once the investor pays a fee. After paying the fee, the investor is left with nothing because the fake crypto coin is worthless, and their original investment was never recovered or returned.

- **Third-party asset recovery companies –** Some companies will offer asset recovery searches for a fee, often thousands of dollars. They use high-pressure techniques to convince people to pay for services that are nothing more than generating a report from publicly available information. They may offer to file a complaint with regulators or find information on the blockchain. In the end, the investor pays an exorbitant fee for actions they can take themselves. Read NASAA's advisory on Third-Party Asset Recovery Companies to find out more.

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

Protect yourself from crypto recovery room scams

- **Contact your regulator –** Victims of crypto investment fraud should resist talking to anyone who offers to help recover lost crypto. Instead, contact your state or provincial securities regulator to file a complaint.

- **Ignore calls, emails, text messages or DMs –** The best way to avoid being manipulated or pressured by a fraudster is to ignore, block and delete their messages. Scammers will move on if you ignore them.

- **Change your contact information –** Changing a phone number and deleting online profiles can be inconvenient, especially now that so many services require you to be online. However, it may ensure that you can't be reached by recovery room scammers who have your past contact information.

- **Be cautious seeking third-party assistance –** There are firms that provide forensic crypto searches. Legitimate firms won't ask for exorbitant or up-front fees without offering anything in return. Before working with anyone, do a thorough background check, including calling your local securities regulator.

- **Do your own research –** Searching the internet and publicly available blockchain information is the best way to determine what happened to your funds. If you've been scammed, it's unlikely that you will recover your lost crypto assets. Be skeptical of anyone who offers crypto recovery services.

The Bottom Line

If you've been contacted by a company or individual offering to help you find lost crypto assets, resist pressure tactics and do your homework. For more tips and information about how to be a better-informed investor, contact your state or provincial securities regulator. Contact information is available on the NASAA website.[3]

2 See https://www.nasaa.org/38322/informed-investor-advisory-third-party-asset-recovery-firms/.

3 See https://www.nasaa.org/contact-your-regulator/.

NASAA has provided this information as a service to investors. It is neither a legal interpretation nor an indication of a policy position by NASAA or any of its members, the state and provincial securities regulators. If you have questions concerning the meaning or application of a particular state law or rule or regulation, or a NASAA model rule, statement of policy, or other materials, please consult with an attorney who specializes in securities law.

To learn more, contact the Investigator on Duty of the ACC Securities Division

602-542-0662 | Info-azinvestor@azcc.gov | azcc.gov/