Learn & Protect

- Fraud Center
- Check Registration & Disciplinary History
- Submit a Tip or Complaint
- RED List
- Office of Proceedings
- Learning Resources
- Materiales Antifraude en Español

English | Español

Don't be Re-Victimized by Recovery Frauds

"We can get your money back."

If you recently lost a portion of your savings or retirement nest egg to a cryptocurrency, forex, or binary options scam, an offer to recover your lost funds may sound very appealing. Unfortunately, for many victims of fraud, the offer may be another scheme that adds insult to injury.

Recovery scams are a form of advance-fee fraud—when you are asked to pay upfront for the chance of getting a much bigger sum of money later. Recovery frauds target victims already harmed by other frauds.

If you've been a recent victim of fraud, be prepared to guard against these follow-on schemes.

Faked News

Recently, a number of scammers successfully gained access to local news websites by using free or low-cost online press release distribution services. Here's how it works:

- The fraudsters create websites posing as fraud recovery investigators. The website is used to solicit fraud complaints, but also includes reassuring customer testimonials, A-plus ratings, and five-star reviews.
- The scammers write a press release about avoiding and recovering from fraud, a break-through technology, or outstanding success record in returning money to victims.
- Links to the scam's website are cleverly planted in the press release. Often the fraudsters are quoted as expert sources.
- The press release is then uploaded to a network of subscribing news outlets.

Many small-town newspapers or community news websites subscribe to these services and automatically post the press releases to complement their locally written news. Likewise, some larger news aggregation websites may subscribe to these automated services to provide broader coverage of business or industry news.

In either case, the fraudsters use creative writing techniques to disarm readers, build hopes, and create a façade of legitimacy. The recovery services are referred to as "fraud recovery experts," or the "one successful way" to get stolen money returned.

When the fraud victims visit the fraudster's website and submit their email addresses and phone numbers for assistance, the scam begins or the victim's personal information is stolen, which could lead to being targeted again in the future. Research indicates that the majority of fraud victims are victimized more than once,[1] and data shows prior victims are often targeted more than nonvictims.[2]

Some published press releases are indistinguishable from other articles on the news website. They'll also sometimes go so far as include references to CFTC advisories, fraud avoidance tips, and links to submit fraud complaints to the CFTC.

Recycling Victims

Another common tactic of recovery fraud is to use existing victim lists. After fraudsters steal victims' money, they also profit from the victims' information—either by hanging onto it for a few months and coming back to run another scam or by selling it on the dark web.

Victim lists can include payment and contact information, personal details, the amount of money taken, and the type of scam that was used.

Commonly, a victim receives a phone call or email from a person claiming to be a government official, an attorney, or recovery service representative. In most cases, the fraudsters claim to have the money already in hand, or are working with the court to distribute the funds. In other cases, the victims are told that the fraudsters who took their money have been tracked down and the caller is notifying victims to begin a civil court action.

Sometimes, victims are told that most or all their money will assuredly be returned if they first pay a small donation, retainer, or overdue taxes. However, after making the first payment, requests for more funds often follow.

How to Identify a Real Government Employee from an Imposter

Imposter frauds are becoming increasingly common. Fraudsters know most people tend to trust law enforcement or government officials, and they use that trust to their advantage. If someone contacts you claiming to be from a court or government agency, there are simple ways you can check:

- If someone calls you claiming to be from the government, write down pertinent information, but **do not confirm personal information about yourself**, including your social security number.
- End the call. Then, call the agency using the contact information on its official website.
- If you receive an email, look at the email domain or any web links that are provided. All government websites and email addresses end in ".gov" or ".fed.us." Only government agencies can get and use these domain extensions.
- Government officials will never use a personal or web-based email account to contact you.
- If the government needs to reach you, they will send official documentation in the mail.
- A government agency will never demand immediate payment or ask for donations.
- Government agencies will not require you to wire money, send prepaid credit or gift cards, use digital assets such as Bitcoin, or make other unusual forms of payment.

Recovery Fraud Warning Signs

Watch for these warning signs. Any of them should be considered a red flag that raises your suspicion. Report any follow-on fraud attempts to authorities.

- You're asked for an email address or phone number before seeing fee disclosures or a detailed list of services.
- You're asked to pay before receiving any service. Be alert to deposits or other seemingly small fees. Sometimes fraudsters ask for small amounts of money at first, but the frequency of requests and amounts increase over time.
- The physical address for the recovery business is not on the website, the address is outside the United States, the address is not found in map or "street-view" searches, or does not appear to be an authentic place of business.
- No phone numbers are provided, or you're asked to communicate through Telegram, WhatsApp, or other messaging platforms.
- You're asked to give bank account details so the "recovered" funds can be deposited directly into your account.
- Calls, letters, or emails are coming from people you don't know or companies you've never contacted.
- The person or organization knows a lot about the money you lost.
- The person or organization is using a web-based email address, such as @Gmail or @Yahoo.
- Organization seals, logos, graphics, or signatures look like they've been cut-and-pasted from other documents.
- The letterhead looks unprofessional.
- There are grammar and spelling errors.
- You are given reasons why the fees can't be taken from the money after it's recovered, or they call the payment a donation or tax.

Also Remember:

- *Never* give personal, payment, or account information over the phone or by email. Even providing an email and phone number could open the floodgates to more fraudulent solicitations.
- Government agencies like the CFTC that prosecute financial fraud will never ask you for money and would only use ".gov" email addresses.
- If an email directs you to a customer service or government website, **don't click the link in an email**. Conduct your own web search for the person or organization and contact them independently.

Victims who are eligible for restitution that is legitimate will likely be notified by mail. If you receive such a letter, verify the information by independently going to the agency's or court's website, or calling them yourself. Do not use phone numbers or web addresses provided in the correspondence until you verify its authenticity. If the communication is part of a fraud, the phone numbers and web addresses will be fraudulent, too. It's good to take precautions, but don't ignore the letter. It could also be real.

Help Fight Fraud – Report Suspicious Activity

Even if you can't get your money back from fraudsters, it's important for all victims to report fraud to help stop others from falling victim to these schemes.

Report frauds to local, state and federal law enforcement and regulatory agencies, including the CFTC. Notifying local, state and federal authorities will also help agencies track frauds, pursue the fraudsters, and warn others. Some agencies, including the CFTC, have whistleblower programs that may entitle you to an award for reporting fraud in some circumstances.

1 Titus, Richard M., and Angela R. Gover. "Personal Fraud: The Victims and the Scams." Crime Prevention Studies 12 (2001): 133-152.

2 Shadel, Doug and Pak, Karla. "AARP Investment Fraud Vulnerability Study," AARP Fraud Watch Network, AARP Research. (2017)

CFTC Headquarters
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
202.418.5000