

CyberGuardLab

Household antivirus, explained

cyberguardlab.com

How to spot a fund recovery scam

Read online: <https://cyberguardlab.com/blog/fund-recovery-scam>

Published October 17, 2026 | Updated October 17, 2026

Short answer

A fund recovery scam is a second con aimed at someone who has already lost money: a "recovery firm," "crypto tracing" service, or self-described law firm promises to get the lost money back, then charges a fee, asks for bank or identity details, or both. The FTC calls these refund and recovery scams and says that if you pay, you lose more money. The FBI has issued repeated warnings about fake recovery companies and fictitious law firms that target cryptocurrency scam victims through social media, messaging apps, search results, and comment sections. This guide explains how the pitch is built, which claims are impossible, and which free channels can actually try to reverse a payment. CyberGuardLab writes these guides independently; a few product pages elsewhere on the site pay us a commission, and that can shape which suites show up in the optional list near the end. Nothing in the checks below costs money, and the paid links sit only in that one labeled section.

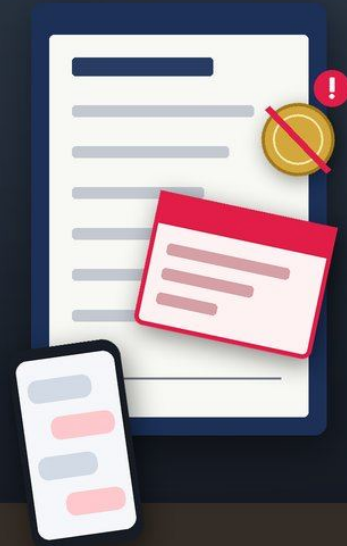
Advertising disclosure: CyberGuardLab is an independent comparison site. We are not TotalAV, Norton, Bitdefender, McAfee, or Avast. If you buy through our links, we may earn a commission, which can affect ranking and placement.

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

CYBERGUARDLAB · GUIDE

How to spot a fund recovery scam

An upfront fee to recover lost money is almost always a second scam.



Short answer

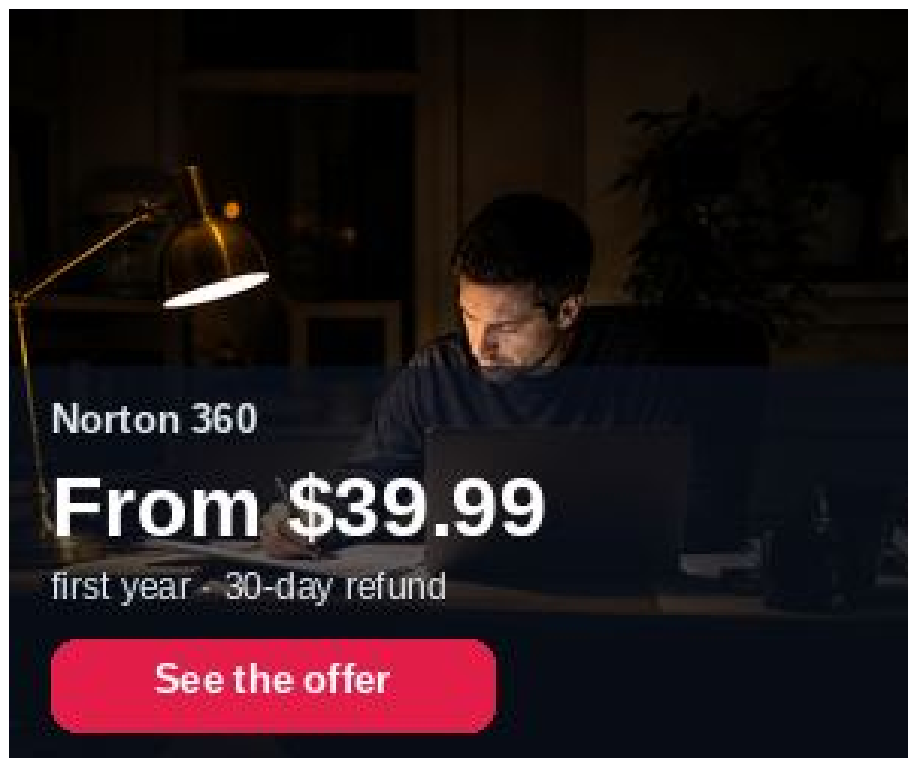
Do not pay anyone upfront to recover money you lost to a scam, and do not give them account numbers, your Social Security number, or remote access. The FTC says anyone who contacts you and asks for an upfront fee to get your money back is a scammer. Government agencies do not charge for help, and the FBI notes that no private company can issue a seizure order for stolen cryptocurrency. The people who can try to reverse a payment are the bank, card issuer, payment app, wire company, gift card issuer, or crypto exchange you used, and you can contact them yourself for free.

Why a past scam makes you a target again

The FTC explains that scammers buy, sell, and trade lists of people who have already been cheated, sometimes with the type of scam, the date, and the amount paid. That is how a stranger can "know" your case. The FBI's August 2025 alert lists the same red flag: a caller who knows the exact amounts and dates of earlier wire transfers and the company you sent money to. Detailed knowledge is not proof of legitimacy; it is proof that your data is on a list.

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

How the recovery pitch usually unfolds

- * The contact finds you, or you find it. A message arrives by phone, email, text, letter, or social media, or you click an ad, a search result, or a comment under a video promising to get crypto back. The FBI's August 2023 alert describes recovery ads in comment sections, search results, and social media.
- * A credible-sounding identity is attached. The caller says they are a law firm, a consumer advocacy group, a "blockchain forensics" team, or a partner of the FBI, CFPB, or another agency. The FBI says there are no law firms that are officially authorized partners of US government agencies.
- * You are told your money has been found. The story may say the funds are frozen, sitting in a foreign bank, or waiting on a "government list of victims." Some versions ask you to open an account at a lookalike bank website to "receive" the money.
- * A fee appears before any money moves. It is called a retainer, processing fee, tax, administrative charge, or "bank verification" deposit. The FBI notes some schemes ask for part upfront and the balance "when funds are recovered."
- * Payment is steered to hard-to-reverse methods. Crypto, gift cards, wire transfers, cash, or a payment app, often sent to a third-party "trading company" for "secrecy." The FTC says only scammers insist on those methods.
- * More fees follow, then silence. You may receive a vague "tracing report," a fake court letter, or a WhatsApp group with supposed bank officers, each step asking for another payment until you stop paying.

Claims a real recovery effort never makes

What the "recovery" contact says | What the official guidance says | What to do

"Pay a retainer or processing fee and we will get your money back." | FTC: anyone who asks for an upfront fee to recover lost money is a scammer | Do not pay; end the contact

"We work with the FBI, CFPB, or FTC on your case." | FBI: no law firm is an authorized partner of a US government agency, and law enforcement does not charge victims | Call your local FBI field office yourself to check any claimed tie

"We can get a seizure order to pull back your crypto." | FBI: private recovery companies cannot issue seizure orders; exchanges freeze accounts only under their own process or legal process | Treat the promise as false

"Your funds are held at a foreign bank; open an account there." | FBI: the bank site in these schemes can look real but is a fraudulent platform | Do not register or deposit

"Pay in crypto, gift cards, or to a third-party company." | FTC and FBI: those payment demands are a scam signal | Refuse every such request

"We guarantee you will get it all back." | FTC: legitimate organizations will not guarantee you will get your money back | Walk away from any guarantee

"Our lawyer can't do video and won't share a license number." | FBI: if a supposed lawyer cannot readily show a license or verify on video, assume they are not legitimate | Verify the license with the state licensing agency

Who can actually try to get your money back

Recovery attempts that can work go through the company that moved your money, not through a stranger. The FTC's What To Do if You Were Scammed page lays out the free routes by payment type:

How you paid the original scammer | Who to contact yourself | What to ask for

Credit or debit card | Your card issuer, using the number on the back of the card or the official app | A refund or dispute of the charge

Bank transfer or Zelle | Your bank or credit union | Reversal of the payment

Payment app such as Venmo, Cash App, or PayPal | The app's own support channel | Reversal and a refund

Wire company such as Western Union or MoneyGram | The wire company | A refund, telling them a scammer tricked you

Gift card | The card issuer, using the number on the card | A refund; keep the card and receipt

Cryptocurrency | The exchange or crypto ATM operator you used | Report the transaction as fraud and ask about reversal

Results vary, and crypto payments lack the legal protections cards have, but none of these routes requires paying a recovery fee to a third party. If you want private legal help, the FBI notes victims can choose civil litigation; find a lawyer through your own search and confirm the license with the state licensing agency rather than hiring someone who cold-contacted you.

How to spot a fund recovery scam

Run these six checks the moment anyone offers to get lost money back.

* Ask who contacted whom. The FBI tells victims to be cautious of firms that contact them unexpectedly, especially when the loss was never reported to anyone. Ads and comment-section posts promising crypto recovery deserve the same suspicion.

* Stop at any upfront fee. A retainer, "tax," processing charge, or verification deposit before money comes back is the core of a refund and recovery scam, the FTC says.

* Test the government claim yourself. Look up the agency's number on your own and call to confirm. Do not use a number, link, or caller ID the contact supplied. Check that the agency even exists; the FBI cites invented bodies such as an "International Financial Trading Commission."

* Verify any lawyer independently. Use the ABA's Lawyer Licensing directory to reach the licensing agency in the state where the lawyer says they practice. The FBI advises asking for license documentation and video verification and assuming the firm is fake if neither comes readily.

* Refuse new accounts, apps, and secret group chats. Do not open an account at a bank you were sent to, install remote-access software, or join a WhatsApp group with "bank processors." These are tools to take more money.

* Go straight to your own payment provider. Contact the bank, card issuer, app, wire company, gift card issuer, or exchange you used for the original payment, using contact details you look up yourself, and ask what they can do.

If you already paid a recovery service

* Contact the company you used to pay the recovery service right away and report it as fraud. For card payments, start with Dispute a fraudulent credit card charge; for app transfers, see Zelle / Cash App payment scam; for gift cards, see Gift card scam.

- * If the "refund" arrived as a check for more than you lost with a request to send back the difference, do not deposit it; that pattern is covered in Fake check scam.
- * If you shared your Social Security number or bank account, follow the recovery plan at IdentityTheft.gov (Report identity theft).
- * If you gave a password or remote access, change that password, sign out other sessions, and turn on 2FA for the account.
- * Report the recovery scam at ReportFraud.ftc.gov (How to report a scam to the FTC) and to your state attorney general. For crypto losses, also file at IC3.gov and include every detail about the "recovery" contact, as the FBI requests.
- * Keep messages, documents, wallet addresses, and call logs. The FBI suggests keeping records of every interaction, including recordings of video chats.

Free habits after any scam loss

- * Expect follow-up contact. The FTC warns that people scammed once are treated as good targets for another pitch.
- * Tell a trusted friend or relative before replying to anyone who mentions your loss.
- * Use only contact details you find yourself for banks, agencies, and law firms.
- * Treat any request for secrecy as a warning, not a safety measure.

What this page is not

This guide is about private "recovery" offers: recovery firms, crypto tracers, and fake law firms that charge a fee to get back money you already lost.

If the contact claims to be an FTC staffer and texts a badge photo, use How to spot a fake FTC employee photo-ID text, which covers that government impersonation in depth. The original crypto loss is explained in Cryptocurrency scam and, for relationship-driven investment cons, in Pig butchering scam. Cash pushed into a crypto kiosk is in Bitcoin ATM cash deposit scam. A tech-support "you were refunded too much" story is a separate trick, covered in Fake refund overpayment scam, and paid "exit" services for timeshare owners are in Timeshare exit scam. This page is general consumer information, not legal advice.

Optional paid security suites

No software can recover money a scammer already took, and none of the steps above needs a paid product. If you also want device or identity protection for the household, these are the only paid links in this guide:

- * Norton plans: higher tiers bundle identity features with device protection (paid link; check the renewal price).
- * Bitdefender plans: a fit when independent lab results lead your comparison (paid link).
- * TotalAV plans: compare by device count and first-year price (paid link; note the renewing rate).
- * McAfee plans: one plan across several phones and computers (paid link; confirm the device limit).
- * Avast plans: practical if Avast is already on your devices (paid link).

You can skip all of them and still follow every step on this page.

FAQ

Are fund recovery services legitimate?

Treat any service that contacts you, or advertises in comments and search results, and asks for an upfront fee as a scam. The FTC says anyone who asks for an upfront fee to get your money back is a scammer.

Can a company really recover stolen cryptocurrency?

Not by itself. The FBI says private recovery companies cannot issue seizure orders, and exchanges freeze accounts only through their own processes or legal process. Report the loss to the exchange you used and to IC3.gov.

Does the FBI or FTC charge a fee to help get my money back?

No. The FBI says law enforcement does not charge victims for investigating crimes, and the FTC says government agencies will never ask for money to help you get a refund.

How did the recovery company know details about my loss?

Scammers buy and trade lists of people who have already been cheated, according to the FTC, and the FBI warns that fake

firms may know exact transfer dates and amounts. That knowledge does not make them real.

How can I check whether a law firm offering recovery is real?

Find the lawyer's licensing agency through the ABA's Lawyer Licensing directory and confirm the license yourself. The FBI advises asking for license documentation and video verification, and treating a firm that cannot provide them as fake.

What should I do first if I already paid a recovery scammer?

Contact the bank, card issuer, app, or exchange you used to pay and report the fraud, then report at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and to your state attorney general. If crypto was involved, also file at [IC3.gov](https://www.ic3.gov).

Sources

- * Refund and Recovery Scams (FTC Consumer Advice)
- * What To Do if You Were Scammed (FTC Consumer Advice)
- * Increase in Companies Falsely Claiming an Ability to Recover Funds Lost in Cryptocurrency Investment Scams (FBI IC3 PSA, Aug 11, 2023)
- * Fictitious Law Firms Targeting Cryptocurrency Scam Victims Offering to Recover Funds (FBI IC3 PSA, Jun 24, 2024)
- * Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds (FBI IC3 PSA, Aug 13, 2025)
- * Lawyer Licensing (American Bar Association)
- * [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud)
- * [IdentityTheft.gov](https://www.identitytheft.gov)
- * Internet Crime Complaint Center (FBI IC3)

Also read

- * Online romance scams
- * Wire transfer romance advance-fee scams
- * Grandparent emergency money scams
- * Fake IRS tax refund scams