C4 × LIONSGATE INTELLIGENCE NETWORK

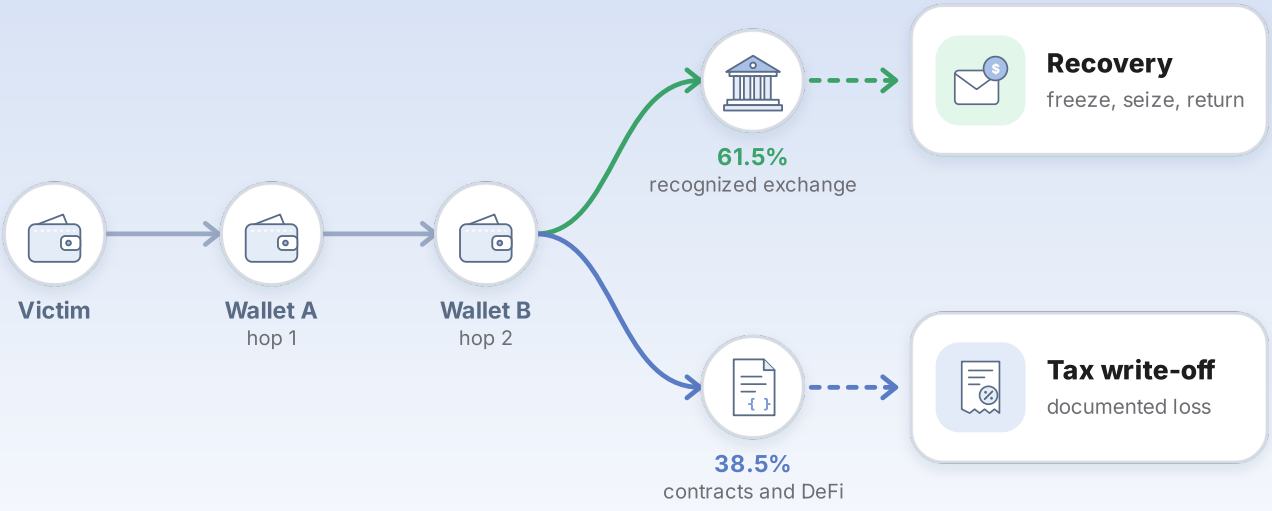
The Recovery Blueprint

For companies and individuals who have experienced financial attacks through online scams

If you've been targeted, there may be options to recover funds or reduce your financial loss.

From one trace to two outcomes

Redrawn from a real Lionsgate Intelligence Network trace



The scale of the problem

Scams are now a trillion-dollar industry

$1 trillion+

lost to scams worldwide in a single year

GASA, Global State of Scams 2024

12,000+

fraud and identity-theft reports filed every day in the U.S. alone

FTC, SEC and FBI IC3, 2025

$15.9B

reported lost by Americans in 2025, up from $12.5B the year before

$7.9B

of that lost to investment scams, the costliest category

4%

of scam victims worldwide say they got their money back

What changed

Built with AI. Delivered through every app.

Scammers use the same AI tools you do. They reach you where you already are: messaging apps, social media, dating apps, marketplaces, job sites and your inbox.



Cloned voices

A few seconds of audio is enough to sound like your CEO or your child.



Deepfake video

Live video calls with faces that don't exist.



Flawless messages

Perfect grammar, any language, written for you.



Instant fake platforms

Trading sites and dashboards built in hours.



REMEMBER

Scams are a global industry run by professionals. Being targeted says nothing about how careful you are.

Foreword

Why we wrote this

C4

At C4, we believe education is an important part of improving cryptocurrency security. Through education, standards, and professional certifications, we work to give people and entities the knowledge and tools to make informed security decisions.

But even strong security practices cannot eliminate every risk. When something goes wrong, people need clear, accurate information about what to do next, what options may be available, and what is realistic.

This guide provides a practical starting point for understanding what may happen after a loss and the questions to ask when considering next steps.

Jessica Levesque

Executive Director, CryptoCurrency Certification Consortium

LIONSGATE INTELLIGENCE NETWORK

Every week we speak with people on the worst day of their financial lives. Many believe there is one way back, or none. Across more than 10,000 cases, we've learned that there is rarely only one.

The exchange, the police, the courts, the bank, the insurer, the tax system: each can be a gate. Our job is to find which ones are open, and to be honest when one is closed.

Eithan Raviv

Founder & CEO, Lionsgate Intelligence Network

About this guide

This guide was developed by C4 and Lionsgate Intelligence Network to provide general educational information about what may happen after a financial scam or cryptocurrency theft and the options that may be available.

Lionsgate Intelligence Network is one provider of cryptocurrency investigation and recovery services. C4 does not endorse or recommend any particular recovery provider, service, strategy, or course of action. This guide should not be interpreted as a recommendation to pursue any specific option.

Recovery, reporting, legal, and tax options vary by country and individual circumstances. This guide includes U.S.-specific information where noted, including U.S. federal tax law. Readers should consult appropriate authorities and qualified professionals based on their circumstances and jurisdiction.

This guide is for educational purposes only and is not legal, financial, tax, or recovery advice. Readers are responsible for evaluating their circumstances and deciding what actions, if any, are appropriate.

Start here

First, breathe. You were targeted, not foolish.



Individuals

You lost crypto to a scam, a hack or an impersonator.



Your company

A business, fund or treasury lost digital assets.



The people who lead it

Founders, executives and finance leads, often targeted next.



Is money still moving? Skip ahead to the checklist on page 25 now. Everything else can wait an hour.

How this guide works

1 **Understand**
What happened, and why it keeps happening — pp. 2–7

2 **Act now**
The first hours, for individuals and companies — pp. 8–10

3 **Recover**
Tracing, your six options, real cases and a timeline — pp. 11–21

4 **Protect**
Avoid the second scam and stay safer — pp. 22–27

Look for the colored tab on the edge of each page to see which part you're in.

The honest truth

Recovery is possible. It is never promised.

Many cryptocurrency transactions are recorded on public blockchains, which can provide investigators with a trail to follow. What matters is where it ends. When it ends at a company that knows its customers, someone can be made to act.



The phrase to remember: “recognized entity”

A business that knows its customers and answers to regulators and courts. Usually an exchange; sometimes a bank, payment company or stablecoin issuer.

- ✓ Checks customers’ ID
- ✓ Can freeze funds
- ✓ Must answer police and courts



Where did it go?

Money at a recognized entity can be frozen where legally and technically possible. Money in an anonymous wallet usually can’t.



How was it paid?

Card and bank payments open doors that crypto transfers can’t.



How fast are you?

Every day you wait, the money has another chance to move.

Anyone who promises your money back is not telling you the truth. That includes people who sound like us.

Companies and people

One attack, two targets

When attackers breach a company, they rarely stop there. The people who sign, approve and decide become the next target, at work and at home.



Why leaders are next

They hold the keys

Signing authority, admin access and personal wallets worth targeting.

The breach exposed them

Emails, org charts, deal pipelines and travel plans are now in the attackers' hands.

They want a fix, fast

Pressure to recover makes a convincing "solution" hard to resist.

REMEMBER

If your company was hit, treat every leader, and their family, as a possible next target in the weeks that follow.

How the attack moves

Eight “initiatives” aimed at decision-makers

The investor

A fund offers bridge money to cover the loss. Its “data room” installs malware or asks you to connect a wallet.

The deal

Acquisition interest, a partnership or a listing. “Due diligence” asks for wallet proofs or a signature.

The job offer

A recruiter with a dream role sends a “skills test” file or app. Opening it hands over the device.

The slow friendship

Pig butchering: weeks of warm chat, then a “can’t-miss” trading platform. Small wins first, then everything.

The urgent call

A voice or video call that sounds exactly like your CEO, CFO or chair. Deepfakes are cheap now.

The authority

Fake police, regulators or exchange compliance send a “freeze notice” and a “safe” wallet.

The rescuer

Once the breach is public, “recovery experts” approach the founders directly.

The side door

SIM swaps, personal email, home devices, family members and personal wallets.

One rule stops most of these. Any request that moves money, keys or access gets verified on a channel you already trust, never the one it arrived through.

For individuals Your first hour

Stop the loss first. The story can wait.

1. **Stop any more money leaving.**
   Move what's left to a brand-new wallet set up on a different, clean device. If a website can spend your tokens, revoke that permission.

2. **Assume your devices may be compromised.**
   Scammers often plant remote-access or fake apps. Do anything sensitive from a different, clean device, and have yours checked once your evidence is saved.

3. **Change your passwords.**
   Email first, then your exchange, banking and social media apps. Use a new, unique password for each.

4. **Turn on two-factor authentication (2FA).**
   Use an authenticator app or security key, not text messages, on every account that offers it.

5. **Go silent, then call your bank and exchange.**
   Never pay a "release fee". Use the word "fraud", and ask about a chargeback or recall today.

6. **Report it.**
   File a police report and, in the U.S., a complaint at ic3.gov. Keep every reference number.

REMEMBER

Speed protects your options. Secure, save, report: in that order, today.

For companies The first hour

Contain the breach. Then protect your people.

1. **Contain.**
   Pause withdrawals and hot-wallet flows, revoke approvals, rotate exposed keys and credentials.
2. **Name one incident lead.**
   Activate your incident and key-compromise plans. One person decides; everyone knows who.
3. **Ask for freezes fast.**
   Alert exchanges where funds landed. For stablecoins such as USDT or USDC, contact the issuer, which may be able to freeze tokens at an address.
4. **Preserve, don’t wipe.**
   Keep logs, signing records and affected devices exactly as they are.
5. **Report and notify.**
   Law enforcement (in the U.S., your FBI field office and IC3), your insurer, which sets notice deadlines, and counsel.
6. **Protect your leaders.**
   Brief executives and their families, lock personal accounts, agree a verification code word, and route every “help” offer through the incident lead.



REMEMBER

Contain the breach, ask for freezes within hours, and protect your leaders. They are often the next target.

Your evidence

One folder. Every option.

Your bank, the police, a lawyer, your insurer and your accountant will all ask for proof. Build it once.

The payments

- [ ] Transaction IDs and wallet addresses
- [ ] Dates, times, amounts, how you paid

The people

- [ ] Names, usernames, phone numbers
- [ ] Full chats and emails with sender address

The platform

- [ ] Website addresses and app names
- [ ] Screenshots of “balances” and fee demands

For companies, also

- [ ] System, access and signing logs
- [ ] Who approved what, and when

Finding a transaction ID

In your wallet or exchange app, open **History**, tap the payment, and look for **TXID** or **Transaction hash**:

```
9f2c51d07a3fe91c…b6d841ab
```

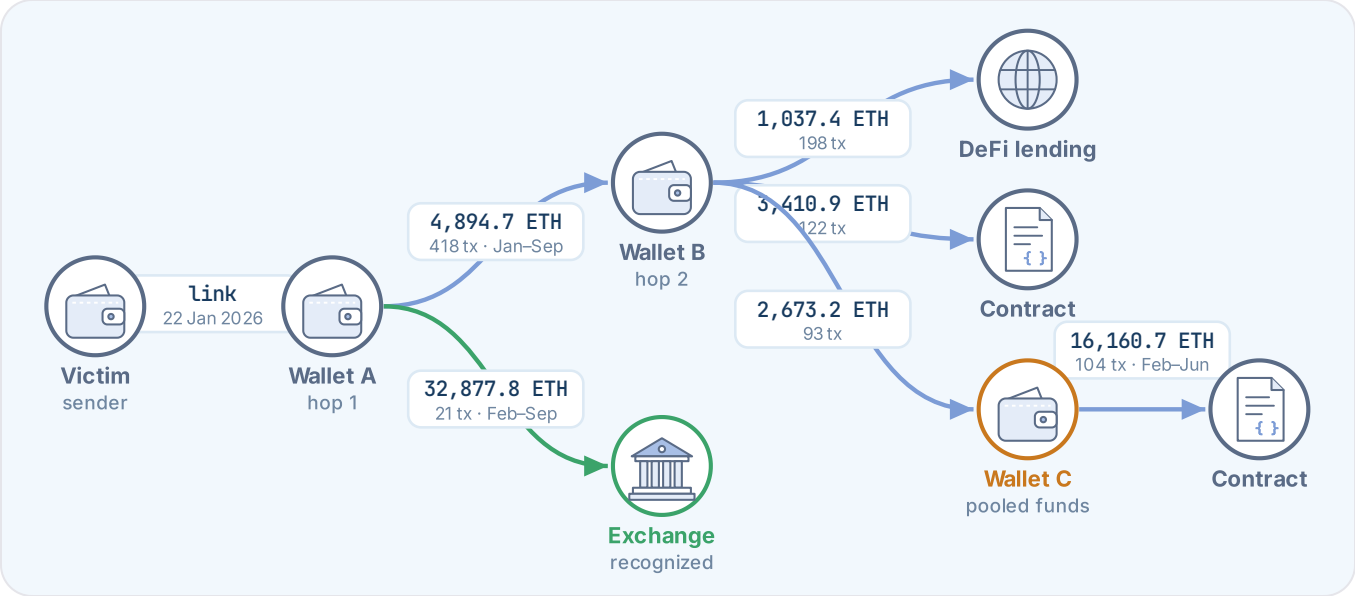
REMEMBER

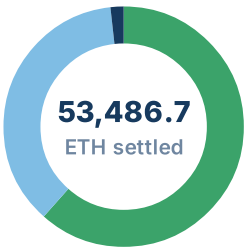
Every recovery option asks for the same proof. Collect it once, keep the originals, delete nothing.

How tracing works

Crypto doesn't disappear. It leaves footprints.

Investigators follow stolen funds hop by hop until they reach a place with a name on the account. Here is what that looks like in a real case.





Where the money settled

- **61.5%** at one recognized exchange
  32,877.8 ETH · a freeze is possible
- **36.6%** in smart contracts
  19,571.6 ETH
- **1.9%** in a DeFi lending protocol
  1,037.4 ETH

Redrawn from a Lionsgate Intelligence Network trace, 2026. Client details and wallet addresses removed. Wallet C also received funds from other sources.

Your options at a glance

Six ways back. Most people only know one.



Freeze it where it landed

1

Exchanges and some stablecoin issuers can lock funds.

Individuals Companies



Let the law seize it

2

Police can seize funds and return them to victims.

Individuals Companies



Take it to court

3

Your lawyer can freeze, unmask and sue.

Larger losses



Pull it back via your bank

4

Chargebacks, recalls and fraud claims.

Paid by card or transfer



Claim on your insurance

5

Home, cyber and crime policies may pay.

Individuals Companies



Recover it through taxes

6

Often overlooked: worth hundreds of thousands for individuals, millions for companies.

Individuals Companies



REMEMBER

These aren't either-or. The strongest cases run several gates at once.

Worksheet · 2 minutes

Which gates are open for you?

Answer five questions. Each answer points you to the options most worth exploring first. On the web version, tap **Check my options** at the top of the page to get your results instantly.

1 Who was affected?

☐ Me, personally ☐ My company

2 How did the money leave?

☐ Crypto transfer ☐ Card ☐ Bank wire or transfer ☐ Payment app

3 When did it happen?

☐ In the last 72 hours ☐ In the last 30 days ☐ Longer ago

4 What kind of scam was it?

☐ Investment or trading platform ☐ Business email or invoice ☐ Impersonation

☐ Hack or account takeover ☐ Not sure

5 Do you have insurance that might apply?

☐ Yes ☐ No ☐ Not sure

IF YOU ANSWERED...	LOOK FIRST AT
Crypto transfer, in the last 30 days	**1 · Freeze it where it landed**
Anything at all	**2 · Report to law enforcement**
My company, or a large loss	**3 · Take it to court**
Card, bank transfer or payment app	**4 · Your bank, today**
Insurance: yes or not sure	**5 · Claim on your insurance**
Investment scam, BEC, or my company	**6 · Tax relief**



REMEMBER

Most cases use more than one gate. Start with a trace and a call to your bank.

Options 1 and 2

Freeze it, or let the law seize it



Option 1

Freeze it where it landed

If a trace shows funds reached a recognized exchange, it can match the deposit to a customer account and lock it. In the trace on page 11, 61.5% of the stolen funds landed at one exchange. Some stablecoin issuers can freeze tokens at the address itself, sometimes within hours. Most act on police or court requests; some act on a well-evidenced report.

YOUR MOVE

Send your evidence report and police case number to the exchange or issuer

TIMING

Hours to weeks, while funds are still there



Option 2

Let the law seize it

Police and federal agencies can seize crypto from exchange accounts and return it to victims through a court-supervised process, such as forfeiture with a victim claim, or restitution after a conviction. Agents have many cases. Clear evidence helps move yours up the pile.

YOUR MOVE

Report, hand over your evidence, file your victim claim when notified

TIMING

Months to years



REMEMBER

A freeze only works while funds are still there. Report early and share your evidence.

Options 3 and 4

Go to court, or go to your bank



Option 3

Take it to court

You don’t have to wait for a criminal case. A lawyer can ask a court to freeze accounts, order an exchange to reveal who owns them, and win a judgment to collect what’s frozen. It costs money, so it suits companies, larger losses, or victims who band together.

YOUR MOVE

See a lawyer who handles crypto fraud, trace report in hand

TIMING

Weeks for a freeze, months for a judgment



Option 4

Pull it back through your bank

If you paid by card, bank transfer or a payment app, ask for a chargeback, a payment recall or a fraud claim. Some countries now require banks to reimburse certain scam transfers. For companies, a fast wire recall can stop a transfer before it settles.

YOUR MOVE

Call your bank today and ask which fraud claims apply

TIMING

Strict deadlines, often days or weeks

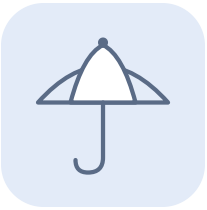


REMEMBER

Courts and banks work on deadlines. Ask today, even if you’re unsure it applies.

Option 5

Check your insurance before anything else



Option 5

Claim on your insurance

For individuals, some home, renters and cyber policies cover theft or fraud. For companies, look at crime policies (especially social-engineering cover), cyber policies and custody insurance. Most people never check, and many policies require notice within days.

YOUR MOVE
Check every policy and notify your insurer promptly

TIMING
Notice windows can be short

What insurers usually ask for

- ✓ Proof the loss happened: transfers, dates and amounts
- ✓ How it happened: the messages, calls and requests
- ✓ Where the money went: a forensic trace
- ✓ Police or IC3 report numbers
- ✓ What you've done to recover it



You may not be the only victim. When many people or companies are hit, there may be group lawsuits, court-run claims or official victim notification programs. Register everywhere you can.

Option 6 · The most overlooked

Recover it through your taxes

When the money can't be traced back, the loss itself can still be worth a great deal. In the U.S., a theft loss can reduce the tax you owe, and sometimes bring back tax you've already paid.

Large individual cases — potential tax savings

Hundreds of thousands

of dollars in tax savings. U.S. taxpayers who lost money in certain scams entered into for profit may qualify for a theft-loss deduction under IRC §165. Eligibility depends on the circumstances, including whether the loss qualifies as theft under applicable law and whether there is a reasonable prospect of recovery.

Companies — potential tax savings

Millions

of dollars in tax savings. U.S. businesses that experience qualifying theft losses, including business email compromise or stolen treasury funds, may qualify for a federal tax deduction. Eligibility depends on the circumstances.

Tax treatment and potential savings depend on the facts and circumstances of each case.

$600,000 qualifying deductible loss

Potential federal tax savings:

up to $222,000*

*Simplified example. Assumes the full loss qualifies for a deduction at a 37% federal tax rate. Actual savings vary by taxpayer.

$50M qualifying deductible loss

Potential federal tax savings:

up to $10.5M*

*Simplified example. Assumes the full loss qualifies for a deduction at a 21% federal tax rate. Actual savings vary by business.

What the IRS needs to see

1. **Proof of theft** and the exact amount lost
2. **Evidence that there is no reasonable prospect of recovery.** A forensic report may be one source of supporting documentation.
3. **The right tax year**, usually the year the loss was discovered

Consult a qualified U.S. tax professional to determine whether a loss qualifies for a deduction. Insurance payouts reduce the deductible amount.

Case study

The recovery gate closed. The tax relief gate opened.

Individual

A 58-year-old project manager, Ohio

Loss	Scam	Gate opened
$240,000	Fake investment platform	Tax relief

1 What happened

A friendly online “mentor” introduced him to a crypto trading platform. Over seven months he moved his savings in and watched the balance grow. When he tried to withdraw, it demanded a “release fee”, then went dark.

> “I thought the only question was whether I’d get my bitcoin back. Nobody told me there was a second question.” C. R., Lionsgate Intelligence Network client

2 Steps taken

Nov 2024	**Report and trace.** Reported to IC3. Funds traced through six hops to an offshore exchange that ignores law enforcement.
Jan 2025	**Recovery assessed.** Eight weeks on, no realistic path to getting the money back.
Feb 2025	**Report to his CPA.** A theft-loss substantiation report documented the loss and that it couldn’t be recovered.
May 2025	**Refund paid.** His CPA claimed the theft loss; the deduction wiped out his 2024 federal tax.

3 The outcome

$38.6k	~$55k	$146.4k
Tax refund	Carried forward	Not recovered

$240k	$38.6k	1
lost	tax refunded	gate opened

The lesson. When the money can’t be traced back, the loss itself can still be worth something.

Illustrative case based on client experiences; details changed. Not a promise of any result.

Case study

One email. $100 million sent. $60.5 million back.

Company

A mid-size company, finance team

Loss	Scam	Gates opened
$100,000,000	Business email compromise	Insurance + tax relief

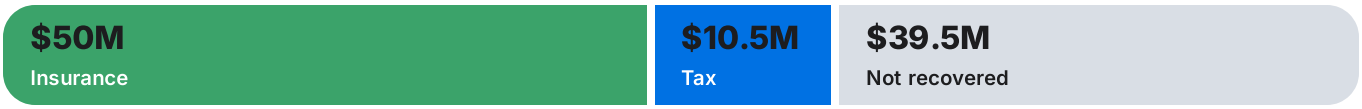
1 What happened

Attackers took over a trusted supplier's email and studied months of real invoices. An invoice with "updated" bank details arrived, followed by a request "from the CEO" to prioritize it. Finance sent $100 million. Within hours it was converted to stablecoins and split across chains.

2 Steps taken

Day 1	**Contain and report.** Incident lead named; FBI and insurer notified the same day.
Day 3	**Trace.** Funds followed through bridges, mixers and offshore services that ignore legal requests.
Week 8	**Recovery status.** A CPA Theft-Loss Substantiation & Recovery Status Report: the funds can't be recovered.
Gates	**Insurance and tax relief.** The crime policy paid $50M; the remaining $50M was deducted as a business theft loss: $10.5M.

3 The outcome



$100M	$60.5M	2
lost	back in value	gates opened

The lesson. Notify your insurer on day one, and document everything. Both gates depend on it.

Illustrative composite based on common BEC patterns. Not a specific client. $50M × 21% federal rate = $10.5M.

Proposed timeline

What a successful recovery can look like

1. **Report and trace** — SAME DAY
   You report the loss. An investigator starts following the money.
2. **Evidence report** — UP TO 7 BUSINESS DAYS
   Every hop, amount and time, written so police and courts can act on it.
3. **Law enforcement investigates and issues a subpoena** — TIMING VARIES
   Working with a forensic firm? Verify it's a legitimate one.
4. **Exchange freeze** — POTENTIALLY HOURS TO DAYS
   The exchange matches deposits to accounts and locks the funds.
5. **Legal order and seizure** — WEEKS TO MONTHS OR LONGER
   A warrant or court order moves the funds into official custody.
6. **Money returned** — MONTHS OR LONGER
   Through a victim claim, restitution or a judgment.
7. **Tax return** — WHEN THE IRS PROCESSES YOUR RETURN
   Any unrecovered loss may still reduce your tax.

Illustrative timeline only. Steps, order, and timing vary by case. Funds may not be recovered.

Being realistic

What can stand in the way

- [ ] **Time.** Money withdrawn before a freeze is much harder to reach.
- [ ] **Mixers and privacy tools** can make tracing and attribution significantly more difficult.
- [ ] **Uncooperative destinations.** Some offshore or unlicensed services ignore every request.
- [ ] **Borders.** When attacker, exchange and victim are in different countries, everything slows.
- [ ] **Missing records.** Without transaction IDs and logs, it’s hard to prove which funds were yours.

That’s exactly why you need more than one option

When one door closes, another may open. In our individual case study, the exchange route closed; the tax route didn’t. A trace that can’t lead to a freeze can still power a bank claim, an insurance claim or a tax refund.

Recovery scams

Don’t get scammed twice.

Fake “recovery experts”, lawyers and police target individuals within days, and founders as soon as a breach is public.

Walk away if they...

- ✕ Contacted you first
- ✕ Promise your money back
- ✕ Ask for seed phrases, keys or access
- ✕ Want a fee to “release” funds
- ✕ Say they can “hack back”
- ✕ Rush you to pay today

A real professional will...

- ✓ Be a company you can verify yourself
- ✓ Tell you what they can’t do
- ✓ Never ask for keys or access
- ✓ Show evidence before claims
- ✓ Work alongside police
- ✓ Give you time to think

Never share a seed phrase or private key. No investigator, exchange or police officer will ever ask for it.

Before you hire anyone

12 questions to ask a recovery firm before you pay

1. Can I verify your company independently: registration, address and real people?
2. Who exactly will work on my case, and what is their background?
3. What will you do, and what can't you do? Can I have that in writing?
4. Do you work alongside law enforcement, or claim to replace it?
5. Will you ever need my seed phrase, keys or wallet access?
   The only right answer is no.
6. How are you paid? Is there a written scope and fee agreement?
7. Do you ask for "release" or "recovery" fees before funds are returned?
8. Can I see a sample report, with client details removed?
9. How will you protect my personal data?
10. What happens if the funds can't be recovered?
11. Who will speak to the exchange, the police and my lawyer?
12. Can I take time to think and get a second opinion?

Walk away immediately from anyone who guarantees results, contacted you first, asks for keys, or wants an upfront fee to "unlock" your money.

Stay safer · with C4

Make yourself, and your company, a harder target

FOR INDIVIDUALS

Seed phrase offline. Paper or metal, never photographed or in the cloud.

Hardware wallet for savings you don't trade.

Check the whole address before you send.

Distrust guaranteed returns.

Slow down. Scams run on urgency.

FOR YOUR COMPANY

Multiple approvers for every significant transfer.

Keys generated and stored to a written standard.

A key-compromise plan, tested before you need it.

Separate personal and work devices for leaders.

Out-of-band checks on every money or access request.

C4 publishes the CryptoCurrency Security Standard (CCSS), an open framework for securing systems that hold crypto: cryptoconsortium.org.

REMEMBER

Most attacks succeed through people, not code. Slow down, and verify on a channel you trust.

Tear out and keep

If it's happening now

FOR INDIVIDUALS

- [ ] Move remaining funds to a new wallet on a clean device
- [ ] Revoke wallet permissions
- [ ] Stop all contact. Send nothing more
- [ ] Change passwords; turn on two-factor
- [ ] Call your bank about a chargeback or recall
- [ ] Tell your exchange it's fraud
- [ ] Save TXIDs, addresses, amounts, times
- [ ] Report to police and ic3.gov
- [ ] Check insurance; tell your accountant

FOR YOUR COMPANY

- [ ] Pause withdrawals and hot-wallet flows
- [ ] Rotate exposed keys and credentials
- [ ] Name one incident lead
- [ ] Ask exchanges and stablecoin issuers to freeze
- [ ] Preserve logs and devices. Don't wipe
- [ ] Report to law enforcement
- [ ] Notify your insurer and counsel
- [ ] Brief leaders and their families
- [ ] Agree a verification code word

Case numbers and contacts

Glossary

Words you'll hear

Seed phrase
A set of words used by many cryptocurrency wallets to back up or recover a wallet. Often 12 or 24 words.

Private key
The secret that signs transactions. Never share it.

Wallet address
A public string that receives crypto, like an account number.

Transaction ID (TXID)
The unique code for one transfer on a blockchain.

Hop
One move of funds from one wallet to the next.

Unaffiliated wallet
A wallet no known company controls.

Deposit address
An address for receiving cryptocurrency. Exchanges may use deposit addresses to associate deposits with customer accounts.

Recognized entity
A business that knows its customers and answers to courts: an exchange, bank or issuer.

Stablecoin issuer
The company behind a token like USDT or USDC. Some centralized stablecoin issuers can block or freeze tokens associated with particular addresses.

Mixer
A service that blends funds to break the trail.

Bridge
A service that moves funds from one blockchain to another.

Subpoena
A legal order requiring a company to hand over information.

Seizure and forfeiture
The legal process by which authorities take and return funds.

Restitution
Money a court orders an offender to repay a victim.

Chargeback
A card payment reversed by your bank.

Theft loss (IRC §165)
A U.S. tax deduction for money lost to theft or fraud.

Business email compromise (BEC)
A scam using a real or faked business email to redirect payments.

Pig butchering
A long, friendly con that ends in a fake investment platform.

Disclaimer

This guide is for general educational purposes only and does not constitute legal, financial, tax, or recovery advice. Recovery options, legal requirements, tax treatment, and outcomes vary by case and jurisdiction. No recovery or tax outcome is guaranteed. Consult qualified professionals regarding your specific circumstances.

Sources and notes

Where the numbers come from

1. **Global Anti-Scam Alliance (GASA) and Feedzai**, Global State of Scams Report 2024. $1.03 trillion lost to scams worldwide in 12 months; 4% of victims reported full recovery. Survey of 58,000+ people.
2. **U.S. Federal Trade Commission**, Consumer Sentinel Network data for 2025, reported March 2026. About 3 million fraud reports and $15.9 billion in reported losses; $7.9 billion from investment scams; $12.5 billion in 2024; plus over a million identity-theft reports a year.
3. **FBI Internet Crime Complaint Center (IC3)**, 2025 Internet Crime Report. 1,008,597 complaints (about 3,000 a day) and $20.9 billion in losses; business email compromise about $3.0 billion. Report at ic3.gov.
4. **U.S. Securities and Exchange Commission (SEC)**, tips, complaints and referrals received each year.
5. **U.S. Internal Revenue Code §165** and IRS Office of Chief Counsel guidance (2025) on deducting losses from scams entered for profit.
6. **C4, CryptoCurrency Security Standard (CCSS)**, cryptoconsortium.org.

About the figures

Reported losses understate the problem: most victims never report. Daily figures are annual totals divided by 365. The 12,000+ daily figure combines FTC fraud and identity-theft reports, FBI IC3 complaints and SEC tips; some victims report to more than one agency. Both case studies are illustrative, based on client experiences and common attack patterns.

Edition and review

Edition	1.0 · October 2026
Tax review	[CPA reviewer, firm]
Legal review	[Attorney, firm]
Next update	October 2027

REMEMBER

You may have more than one option.

Your savings or your company's treasury. Move fast, keep the proof, follow the money, and trust evidence, never promises.



START WITH A FREE CASE ASSESSMENT

www.lionsgate.network

Lionsgate Intelligence Network traces stolen crypto and prepares evidence for individuals, companies, lawyers, accountants and law enforcement. We never ask for your keys. We never guarantee results.

C4

The CryptoCurrency Certification Consortium publishes the CryptoCurrency Security Standard (CCSS), education and certifications for safer crypto.

cryptoconsortium.org

LIONSGATE INTELLIGENCE NETWORK

Lionsgate Intelligence Network is a blockchain forensics firm that traces stolen digital assets for victims and law enforcement.

lionsgate.network

General education only, not legal, financial or tax advice. No one can guarantee recovery of lost funds or any tax outcome. Options and deadlines vary by country and case. Case studies are illustrative. © 2026 C4 and Lionsgate Intelligence Network.