Recovery After a Scam

Recovering from Scams

Additional information and resources about recovering from a scam can be found in the [Financial Scams Reporting] guide.

Use this guide if money, accounts, or personal information have already been compromised and you need clear next steps to limit damage, recover funds where possible, and protect yourself from follow-on attacks.

This guide covers:

- Recovering money from cyber scams
- Credit freezes and fraud alerts
- Bank, card, and platform reporting
- Evidence collection and documentation

If there is an immediate threat to your safety, call 911.

Recovery – Do This First

Stop the Bleeding

- Act immediately to prevent additional losses.
- Stop all payments and communication with scammers
- Do not send more money to “recover” losses
- Do not respond to follow-up messages or calls
- Expect “recovery scams” claiming they can get your money back

Secure Your Financial Accounts

Using official phone numbers (not links or numbers provided by messages):

- Contact:
  - Banks and credit unions
  - Credit/debit card issuers
  - Payment apps (Zelle, Venmo, Cash App, PayPal)
- Report the activity as fraud
- Ask about:
  - Chargebacks or reversals (time-sensitive)
  - Freezing or securing accounts

- Issuing new cards or account numbers
- Request case or reference numbers
- Many recovery options expire within hours or days.

Secure Online Accounts (From a Safe Device)

Email is often the gateway to everything else.

- Change passwords for:
  - Email accounts
  - Banking and payment apps
  - Social media
  - Shopping and subscription accounts
- Log out of all active sessions
- Review and update:
  - Recovery email and phone numbers
  - Authorized devices and app connections

Recovering Money After a Scam

What May Be Recoverable

- Credit card charges (often best chance)
- Pending bank transfers
- Unauthorized transactions reported quickly

What Is Often Hard to Recover

- Cryptocurrency transfers
- Gift cards
- Wire transfers sent and completed
- Peer-to-peer payments voluntarily sent

Even if recovery seems unlikely, reporting still matters for investigations and victim protection.

Credit Protection & Identity Safeguards

Place a Fraud Alert or Credit Freeze

If personal data was exposed:

- Contact credit bureaus to place:
  - Fraud Alert (alerts lenders to verify identity), or
  - Credit Freeze (prevents new credit being opened)

- This helps prevent identity theft following scams.

Monitor Credit and Accounts

Review bank and card statements daily for several weeks

- Check credit reports for:
    - New accounts
    - Address changes
    - Hard inquiries you didn't request

Evidence Collection & Documentation

Preserve Everything

Create a dedicated folder (digital or physical) and save:

- Screenshots of:
    - Messages, emails, texts
    - Ads or fake websites
    - Payment confirmations
- Records of:
    - Dates and times
    - Amounts sent
    - Account names and usernames
    - URLs and phone numbers
- Case numbers from:
    - Banks
    - Platforms
    - Law enforcement

Do not delete evidence until reporting is complete.

Report the Scam

- National Reporting
    - Federal Trade Commission (FTC)
        - Main federal agency for consumer fraud
        - reportfraud.ftc.gov
    - Internet Crime Complaint Center (IC3) – FBI
        - Tracks internet-based financial crimes and scams
        - ic3.gov
    - U.S. Postal Inspection Service

        - If the scam involved mailed checks, money orders, or parcels
        - uspis.gov/report
    - Secret Service Cleveland Field Office
        - Main federal agency for financial crimes
        - 216-750-2058
- Ohio Resources
    - Ohio Attorney General – Consumer Protection & Identity Theft
    - https://www.ohioattorneygeneral.gov
    - Consumer Protection Hotline: 800-282-0515
- Geauga County
    - Geauga County Sheriff's Office
    - https://www.geaugasheriff.org
    - Local police non-emergency line for documentation
    - Call 911 if threats, coercion, or immediate danger are involved

Police reports can support disputes, insurance claims, and future protection.

Watch for Follow-Up & Recovery Scams

After an incident, scammers often return pretending to:

- Be law enforcement
- Be fraud departments
- Offer paid "recovery services"

No legitimate agency charges fees to recover scam losses.

Do not engage. Verify independently.

Emotional & Crisis Support

Being scammed can cause shame, fear, anger, or distress. These reactions are common and valid.

- 988 Suicide & Crisis Lifeline
- Call or text 988 (24/7, confidential)

Support is appropriate, scams are designed to manipulate.

Recovery – Ongoing Protection

- Keep all reports and case numbers together
- Revisit account security regularly

- Expect increased scam attempts for a period of time
- Lean on trusted people, do not isolate
- Recovery is a process, not a single step.

How to Reduce Future Risk

- Slow down, urgency is the scammer's tool
- Verify requests independently
- Never send money to "fix" a problem
- Treat unexpected contact as suspicious
- Ask for a second opinion before acting
- Add a Trusted Contact to all financial accounts