

Financial Scam Recovery: What to Do, Who to Call, and How to Heal



By Ally Armeson, Executive Director, FightCybercrime.org

Scams are everywhere—texts, emails, fake alerts, and more. Some scammers can even use technology to replicate the voice of a loved one in distress. We hear about them all the time. But what happens after the scam? Can you get your money back? What should you do next?

The truth is, recovery depends on how much was stolen, how the money was stolen, and how fast you act. And while some frauds are easier to recover from, others leave lasting emotional and financial scars. If you've been affected by a scam, or want to be ready just in case, here's what recovery really looks like.







What We'll Cover

- How to Handle Small Scams
- How to Handle Large Scams
- Emotional Recovery

First, How to Handle Small Scams

If a small amount is stolen—maybe \$10 or \$500—you may have a chance to recover some or all of it, especially if you used a credit card. These frauds are often one-time events, such as fake charity donations, toll-alert scams, or fraudulent tech-support calls. They typically involve credit cards, debit cards, payment apps such as Venmo or PayPal, or gift cards.

Most Commonly Reported Scam In 2024

-  Government imposters
-  Tech support scams
-  Online shopping scams
-  Business/job opportunity scams
-  Investment scams
-  Internet services scams

Government imposters surged from \$171M in 2023 to \$789M in 2024.

Source: \$12.5 Billion Reported Lost to Scams and Fraud in 2024, Older Adults Hit Hard, AARP, 3/12/25

Credit Cards Offer the Strongest Protections

If you report the fraud quickly to your card issuer or bank—ideally within 72 hours—they will likely refund the charge after a brief investigation. For instance, if a scammer uses your credit-card details to make an unauthorized online purchase and you report it promptly, your card issuer will usually reverse the charge after confirming the fraud.

Debit Cards and Payment Apps: Slower and Less Certain

Debit cards and payment apps offer limited fraud protection, so the likelihood of getting your money back is much lower than credit cards. If you report fraud quickly, your bank may reverse a debit-card charge, though it can take longer than credit-card disputes.

With payment apps such as Venmo or PayPal, refunds are rare if you authorized the payment—even under false pretenses—because these apps treat transactions like cash. Your best chance is to report the scam immediately to the app and your bank.

With Gift Cards, It's Tough to Get Your Money Back

Scammers impersonate trusted individuals—such as family members or charities—through email, text, phone, or social media. Instead of requesting cash, they pressure victims to purchase gift cards for seemingly legitimate reasons such as paying fees or helping someone in need. Victims are then asked to share the card codes, enabling scammers to spend or resell them.

Once the card number and PIN are shared, scammers usually drain the balance immediately. Most retailers won't refund a gift card that's been used—even if you report the scam. Your best chance is if the card hasn't been redeemed yet and you act fast by contacting the issuer.

Stop Identity Theft Before It Starts: Freeze Your Credit

Freezing your credit means locking your credit report so lenders can't open new credit cards or loans in your name without your permission. This step is especially effective against identity-theft scams, where criminals try to open accounts using your personal information—for example, applying for a new credit card under your name and mailing address.

It's free and can be done online or in the apps for Experian, TransUnion, and Equifax. After creating an account, you can freeze your credit instantly—with a single tap in the app—and lift it just as easily when you need to apply for credit.

The Biggest Mistake We See in Small-Dollar Scams: Waiting Too Long

Many people put off reporting to their bank because it feels like a hassle for “just \$50” or “just \$100.” But the sooner you act, the better your chances of getting your money back—especially if you used a credit card or debit card. Quick reporting can stop scammers from draining more funds and gives banks the best chance to reverse charges.

Second, How to Handle Large Scams

Scams involving thousands—or even millions—are devastating. They often involve romance scams, investment fraud, house-title theft, or courier scams, and typically use wire transfers or cryptocurrency for speed and anonymity. Once money moves, recovery is almost impossible. Banks may freeze funds if reported within hours, but scammers move fast, often across borders.

So, what can you do?

- Stop communicating with the scammer immediately
- Document everything: messages, emails, transactions
- Contact your bank and ask them to block accounts, initiate a dispute if possible, and monitor for suspicious activity
- Report the scam to www.ic3.gov and local law enforcement

Why report if recovery is unlikely?

Reporting helps law enforcement connect cases, influence policy, and protect others. In rare cases, victims recover part of their funds—but usually only when scams are reported quickly and are tied to larger investigations. It's also important to be cautious of “recovery scams” that promise to get your money back for a fee.

Recovery scams target fraud victims by promising to retrieve stolen money for an upfront fee. Scammers often pose as law enforcement, government agencies, or recovery specialists. After the fee is paid, they disappear—no funds are recovered, and the victim has had more money stolen from them. Key warning sign: Legitimate agencies never charge upfront fees for recovery.

Most Crucial Step in Large-Dollar Scams

Facing what happened is incredibly difficult—especially when scammers use highly sophisticated tactics to build trust and keep you engaged. Stopping communication is a crucial step towards breaking the criminal's control, but recovery really begins when you reach out for support and realize what happened to you was a crime and not a personal failure.

Third, Emotional Recovery

Research found that nearly half of scam victims experience sleep problems, and about one in four suffer panic or anxiety attacks after the crime. These aren't just stress responses—they're signs of trauma.¹

People often downplay their experience: "It was only \$50," or "I should've known better." They do this because shame and self-blame are powerful silencers, and admitting the full impact feels overwhelming. Even small amounts stolen can shake your confidence.

The emotional toll after a fraud can be profound. Victims often describe grief, isolation, and a loss of trust—not just in others, but in themselves. Some scams are especially cruel because they build a relationship over time—romantic, professional, or friendly—and then exploit it. They don't just take your money—they erode your sense of security and self-trust.

Finding Your Footing After a Scam

Unfortunately, financial recovery isn't always possible—but reclaiming your peace of mind is. Here are three steps that can help you start healing.

1. Start by Letting Go of Self-Blame

Your trust was exploited—not your intelligence. Feeling shame or self-blame is common but misplaced. Remind yourself:

"This wasn't about being careless; it was about being human."

Acknowledging this truth helps reduce isolation and start healing.

2. Seek Support and Guidance

You don't have to navigate recovery alone. FightCybercrime.org offers resources such as private peer groups and counselor-led sessions for victims of confidence scams. These programs provide a safe space to share experiences, rebuild trust, and learn practical steps for regaining control.

3. Take Back Control Through Prevention

One of the most empowering steps after a scam is reducing the risk of it happening again. Start small:

- Freeze your credit to block new accounts in your name
- Change passwords and enable multi-factor authentication
- Consider identity monitoring services to catch suspicious activity early.

These actions restore a sense of security and confidence, which is key to emotional recovery

Know These Common Scam Types

- **Romance Scam:** A fraudster pretends to be a romantic partner online, builds trust, and then asks for money—often for fake emergencies or travel.
- **Investment Fraud:** Scammers promise high returns with little risk, often through fake investment opportunities or cryptocurrency schemes.
- **House Title Theft:** Criminals steal your identity to transfer your home's title into their name, then take out loans against the property.

To Summarize

First, small-dollar scams are often recoverable—but only if you act quickly. Second, large-dollar scams may not lead to financial recovery, but reporting it can help law enforcement build cases and prevent others from being targeted. Third, emotional recovery can matter just as much as financial recovery. Victims often experience deep feelings of shame and isolation, and they need support.

From Shock to Strength

Scam recovery starts with shock. Whether it's \$50 or \$50,000, the moment you realize your money has been stolen is gut-wrenching. But recovery isn't just about stolen money, it's about protecting your future, emotionally and financially.

Give yourself permission to focus on healing. Healing begins when you stop blaming yourself and start rebuilding. And you don't have to do it alone.

Next Steps

1. Freeze Your Credit

Freezing your credit is free, reversible, and easy to do online or in the apps for Experian, TransUnion, and Equifax. After creating an account, you can lock your credit instantly and lift it just as easily when needed.

2. Get Expert Guidance About Scam Recovery

Visit <https://fightcybercrime.org> for step-by-step instructions and additional recovery resources, including emotional support and scam-reporting tools.

3. Use Monitoring Services

Consider identity and financial-monitoring tools such as EverSafe, Aura, or IdentityForce. These services send alerts for suspicious activity so you can respond quickly.



Ally Armeson, Executive Director, FightCybercrime.org

At FightCybercrime.org, Ally leads national initiatives to help people recognize, report, and recover from cybercrime. A former U.S. Army service member, she spent a decade managing humanitarian and recovery programs worldwide. Her military experience shaped a lifelong mission to protect communities from exploitation. For the past four years, she has focused on restoring dignity and digital safety for victims of online crime—ensuring no one recovers alone.

Source:

¹ Taking care of your health after identity theft, Allstate, 9/29/25

Hartford Mutual Funds may or may not be invested in the companies referenced herein; -however,- no particular endorsement of any product or service is being made.

Links to a non-Hartford Funds site are provided for users' convenience only. Hartford Funds does not control or review these sites nor does the provision of any link imply an endorsement or association of such non-Hartford Fund sites. Hartford Funds is not responsible for and makes no representation or warranty regarding the contents, completeness or accuracy or security of any materials on such sites. If you decide to access such non-Hartford Funds sites, you do so at your own risk.

Ally Armeson is not affiliated with Hartford Funds. This material is for informational purposes only.

Hartford Funds Distributors, LLC, Member FINRA. MAI468 1225 5032718