

Financial Fraud Trends

& Your Fraud Protection Checklist

Financial fraud continues to evolve, becoming increasingly sophisticated and difficult to recognize. Scammers are using artificial intelligence, social engineering tactics, and compromised personal information to make fraudulent communications appear authentic.

In 2024, consumers reported approximately \$12.5 billion in losses to fraud, according to the Federal Trade Commission (FTC). Knowing common fraud tactics can help you spot warning signs and protect yourself and your finances.

Fraud Trends to Watch For

AI Voice Cloning and Video Deepfakes

Artificial intelligence now makes it easier for criminals to mimic real people's voices and appearances. Using only a short social media video, voice message, or recorded call, a scammer may be able to create a convincing voice imitation.

Deepfake technology can also be used to create realistic video or audio communications. A fraudster may impersonate a family member, coworker, financial professional, or other trusted individuals and use the false identity to persuade someone into sending money or disclosing sensitive information.

How to Protect Yourself:

- Treat unexpected requests for money or personal information with caution, even when they appear to come from someone you know.
- Avoid sharing unnecessary personal information or voice recordings publicly.
- If a request seems unusual, end the conversation and call the person back using a trusted phone number.
- Establish a family passphrase that can be used to verify someone's identity during an unexpected emergency.



"Protective Transfer" Scams

In a protective transfer scam, criminals convince victims that their money is in danger and instruct them to move funds to a "secure" account. They may claim that the victim's account has been compromised, that suspicious activity has been detected, or that a package or payment is being held. These scams often rely on fear and urgency. The goal is to prevent the victim from taking time to verify the situation before transferring money.

How to Protect Yourself:

- Remember that legitimate financial institutions will not instruct you to transfer your money to another account to "protect" it.
- Be especially cautious when someone pressures you to act immediately.
- Stop the conversation and contact your financial institution directly using the phone number on your debit card, credit card, or account statement.

Account Takeovers

Account takeovers occur when criminals gain access to an individual's online banking, email, or other accounts via stolen passwords, data breaches, malware, or phishing attacks. They then try to trick you into sharing verification codes, so they have full control of your account.

How to Protect Yourself:

- Create strong, unique passwords for each account and use a reputable password manager.
- Enable multi-factor authentication whenever it is available.
- Never provide a one-time verification code to someone who contacts you unexpectedly.

Synthetic Identity Fraud

This type of fraud involves creating a fabricated identity by combining legitimate information with false details. For example, a criminal may use a stolen Social Security number along with a fake name, address, or other identifying information to establish a new identity.

How to Protect Yourself:

- Review your credit reports regularly and look for any unfamiliar accounts, inquiries, or personal information.
- Consider placing a credit freeze with the three major credit bureaus if you are not planning to apply for new credit.
- Safeguard your Social Security number by only providing it when necessary to legitimate organizations.

Investment and Romance Scams Enhanced by AI

Artificial intelligence is giving scammers new ways to make investment and romance scams appear credible. Criminals use AI to create convincing online personas, generate fabricated testimonials, and produce false investment statements or screenshots showing nonexistent profits.

How to Protect Yourself:

- Be suspicious of investment opportunities involving cryptocurrency.

- Independently verify investment professionals and firms through trusted sources, rather than relying on information sent to you.
- Be cautious with new relationships that quickly request financial assistance.

Email and Invoice Fraud

Emails and invoice fraud can occur when criminals gain access to legitimate business communications or impersonate someone involved in a financial transaction.

How to Protect Yourself:

- Verify payment instructions by calling the intended recipient using a trusted phone number.
- Be extra cautious of last-minute requests to change account numbers or wiring instructions.

Fraud Prevention Checklist

Protecting your money starts with a few consistent habits:

- 1. Slow down when you feel pressured.**
Scammers often create a sense of urgency to prevent you from thinking through a request.
- 2. Verify information independently.**
Locate contact information through a trusted source and reach out directly.
- 3. Secure your accounts.**
Use strong, unique passwords and enable multi-factor authentication whenever possible.
- 4. Recognize common warning signs.**
Requests involving wire transfers, gift cards, and cryptocurrency should be met with scrutiny.
- 5. Report fraud as soon as possible.**
If you send money, disclose sensitive information, or believe an account has been compromised, contact your financial institution and report the incident immediately.