ENDEAVOR

How Successful Families Can Protect Themselves from Fraud

Successful individuals and families are often targeted by sophisticated fraud schemes that can be both financially and emotionally costly. Criminals see opportunity in the complexity of your financial life, the size of your accounts, and the assumption that you may delegate elements of your finances to others.

Protecting your wealth goes beyond market strategies and estate plans. It includes staying vigilant against the ever-evolving landscape of fraud.

By J. Adam Brennen CFP®, CPWA®, CWS® | Partner & President

Common Types of Fraud

Fraudsters are becoming increasingly creative and convincing, often combining technology with old-fashioned manipulation. According to the FBI's Internet Crime Complaint Center, reported internet crime losses reached a record high of $16.6 billion in 2024.[1] These are just the attacks we know about; unfortunately, many go unreported.

Here are some of the **most common scams** targeting affluent individuals and families that we're seeing today.

SIM swap scams:
Fraudsters steal your mobile number by impersonating you with your carrier and then transferring your number to a new SIM card. Once they have your number, they can intercept texts and calls, allowing them to bypass two-factor authentication and gain access to other sensitive accounts.

Tax fraud scams:
Criminals may pose as IRS agents or tax preparers to extract funds or personal information. These scams often include threatening calls about fake penalties or promises of inflated refunds in exchange for Social Security numbers.[2]

Business Email Compromise (BEC): In 2023 alone, the FBI received over 21,000 BEC complaints, with losses totaling more than $2.9 billion. Criminals infiltrate business email systems — often posing as trusted partners or family members — to trick victims into wiring funds to fraudulent accounts.

Investment scams:
From unregistered securities to fraudulent private deals, scammers target high-net-worth individuals with investment pitches that sound legitimate but are designed to separate you from your capital.

Account takeovers:
If criminals gain access to your email, phone, or passwords, they may attempt to hijack brokerage, banking, or crypto accounts — sometimes without triggering alerts until significant damage has been done.

How to Protect Yourself and Your Family

Fortunately, there are effective strategies to reduce your exposure to fraud and respond quickly if something seems off.[3]

Strengthen your digital security

- Use complex, unique passwords and change them regularly. A 6-character password can take from less than 1 second to a few minutes to crack with today's computing power. Increasing the password to 12 characters, combining uppercase, lowercase, numbers, and special characters, could take centuries to crack.
- Sign up for a password manager, such as LastPass, to generate, store, and securely track your login details.
- Install up-to-date anti-virus and anti-spyware programs on your home computers, use a personal firewall, and download software/operating systems updates regularly.
- Implement multifactor authentication (preferably app- or hardware-based rather than SMS).
- Ask your carrier to add a SIM lock or eSIM protection to prevent unauthorized transfers.

Limit your exposure

- Be vigilant against Phishing and Spear Phishing emails and texts. Avoid clicking links in any email or text, no matter how urgent it appears.
- Avoid publicly associating your name with assets, entities, or residences when possible.
- Ensure all financial communication occurs through encrypted, verified channels.
- Use a dedicated device or secure portal for financial transactions when possible.

Work with a secure, trusted financial team

- Confirm that your tax preparers, advisors, and attorneys are all using secure systems.
- Confirm all requests for wire transfers, changes to account instructions, or unusual financial activity on the phone with a phone number listed on the company's website — even if they appear to come from someone you know.

Monitor your accounts proactively

- Review statements regularly and set up alerts for large or unusual transactions.
- Consider freezing your credit or enrolling in professional monitoring services.
- Request an IRS Identity Protection PIN (IP PIN) to help prevent fraudulent tax filings.

Be Prepared

It's an unfortunate reality that part of managing wealth is managing security risk. Protecting your legacy means more than growing your assets. It means guarding against threats that could undo what you've worked so hard to build.

If a security breach does occur, have a plan in place. Fast communication and swift action can limit the damage and improve the likelihood of recovery.

If you're concerned that your accounts may have been compromised — or if you want a second opinion on the strength of your financial defenses — we're here to help. Reach out to your Endeavor team to discuss.

Together, we can keep you one step ahead.

endeavor-advisors.com

[1] FBI's Internet Crime Complaint Center (IC3), 2024 Internet Crime Report. www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[2] Federal Trade Commission, Tax-Related Identity Theft. www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0122-tax-idtheft.pdf

[3] McGriff, Top 3 Fraud Risks for High-Net-Worth Families. www.mcgriff.com/resources/articles/top-3-fraud-risks-for-high-net-worth-families/