



Fraud Protection Across an Evolving Threatscape

Scams are a growing business that is becoming more difficult to deter every day; adaptation and simple fixes can improve your odds.

Anthony DeSantis
Chief Information Security Officer

The news stories appear with alarming frequency and increasing variety: A professional loses thousands of dollars after an account hack; a real estate investor approves altered wiring instructions that funnel payments to a strange account; a grandparent sends money to a “good Samaritan” claiming to help a grandchild out of a jam; bad actors pretending to be law enforcement convince a retiree to hand over cash, gold, gift cards or cryptocurrency to avoid prosecution for made-up crimes. What do the examples have in common? The use of deception to prompt victims to provide key information and ultimately steal their money—sometimes in substantial amounts.



A person is seen from behind, sitting at a wooden desk in a dark room. A desk lamp is turned on, illuminating the desk surface. On the desk, there is a red cup, a white mug, and some papers. The person is wearing a dark long-sleeved shirt. The background is dark, with a window showing some light outside.

Supercharged by connectivity and new artificial intelligence capabilities, online fraud incidents are accelerating rapidly. According to the FBI, last year saw \$20.9 billion in reported U.S. losses, up 26% from \$16.6 billion in 2024. Of these, victims over 60 accounted for \$7.7 billion, up 60% in a single year.

What accounts for the acceleration? In part, it's a function of our current "online, all the time" culture, where many interactions—business and personal—take place electronically and without the natural slowing influences of manual paperwork and bureaucratic inertia. It has also been supported by advances in artificial intelligence, which is maximizing scammers' speed of operation and making it harder to detect potential fraud attempts. Finally, it reflects a new marriage of technology and personal touch to capitalize on individual vulnerability.

Understanding the Trends

Amid the surge in fraud attempts, their nature and emphasis have changed significantly:

Shifting economics. Although companies have historically been the main focus of attacks, fraudsters have found that it can be more cost-efficient to target individuals. Meanwhile, the old "tells" of an email phishing attack are largely gone; typos, bad grammar and the use of a wrong logo, to name a few examples, can all be fixed almost at no cost by AI. Worse, the messages are now often tailored, because AI can assemble an array of information about a given person very quickly. To judge its authenticity, you can no longer rely on the fact that a message sounds real or that the sender knows where you went to college or where you vacationed last week.

Focus on the person. Criminals have recently shifted their focus from breaking into devices to gaining access to your accounts or persuading you to move the money yourself. The reason? It is far cheaper to convince you to make a transfer than to compromise your device and then figure out how to steal from you. What this means is that digital levers often do not constitute the attack, but rather the research and preparation that can make the attack successful. Through digital reconnaissance, criminals can build a sophisticated con—with an array of actors pretending to be, for example, a bank's fraud department, a federal agent or a courier to pick up payment. While entry may come through digital means, the actual attack may rely on personal manipulation—an ironic twist in a technological era.

Stepping back, the net result is an environment where fraud can come from an array of angles, often via emails, texts and data theft, but also through more traditional means. The list of "Common Scams" on page 5 shows the sheer variety of threats to watch for.

What to Do

What can you do to protect yourself online and elsewhere? We've covered cybersecurity [in the past](#),¹ and the good news is that many of our previous suggestions remain worthwhile. Keeping your computer software updated, using multifactor authentication, making passwords (and ideally passphrases) complex, being cautious about what you share online, avoiding clicking on strange email links, pausing before moving ahead with any "urgent" financial request, independently verifying communications from financial providers and more all make sense. However, given the technological advances and increasingly aggressive nature of fraudsters, there are some ideas we want to emphasize:

Limit your AI 'attack surface.' There's a lot to like in AI, but to get the most out of it, people often input very personal financial information—from illness to tax details—and don't worry about the impacts. Unfortunately, AI capability can outpace the tools that protect it; if you don't want something to be retained somewhere else in the world, and then improperly used by others, don't put it into AI.

Another issue relates to the authority you provide to AI agents to assist you in daily tasks. Such agents are often unable to distinguish your instructions from those that may be hidden by scammers in materials (such as emails) that they read on your behalf, and may even act upon them if allowed. The takeaway? Treat an AI agent as a capable but naïve assistant with no instinct for fraud. Research and drafting may be useful, but avoid giving the agent credentials on financial accounts or permission to complete payments without your review.

Verify communications independently, never through the channel where they arrived. Even if you think a communication is real, you should not interact with the email, text or phone number you were provided in the initial outreach, but go to the official source. For example, if you receive a call saying that your credit card was compromised, hang up and call the number on the back of the card. If a financial firm contacts you, go to its website and call the number shown there. Financial firms are frequently impersonated—fake offerings on social media, counterfeit websites, realistic documentation—and it often only comes to light after someone has an issue.

Create a safe word. This is a fix that parents often teach their children in a different context: "If a stranger shows up at school pickup saying your mother's been in an accident, they have to

¹ DeSantis, Anthony, "Cybersecurity in Focus," *Neuberger Wealth Aspire*, Fall 2024; Neuberger, "Protecting Your Personal and Financial Information," April 2026.

Red Flags

Fear or urgency. Scammers try to capitalize on your anxiety by asking for immediate action. Pause and verify the contact independently before you take any action.

Secrecy. Criminals often seek to isolate their victims through manipulation or threats. Never be reluctant to share your issue with advisors or law enforcement.

Requests for information. A common method of gaining access to your personal information in order to facilitate identity theft and/or theft from your accounts.

Offers that are too good to be true. Fraudsters often solicit funds in advance of your receiving your “prize.”

Unexpected checks or electronic fund transfers. Sometimes criminals will ask you to return a portion of the funds via wire transfer, after which you find out that the original payment was fraudulent.

Solicitation via chat groups. Reputable financial providers will not conduct business outside of formal channels.

Common Scams

- **Family crisis:** Scammers call or send an email posing as a family member in distress who needs money immediately. With AI, 10 seconds are enough to clone a voice—and make the call seem especially convincing.
- **Remote access:** A “computer support specialist” calls, pretending that you have a virus or other issue, with the goal of accessing your computer—either to make you pay for the “fix” or to sweep for your financial passwords and other information.
- **Romance scams:** Fraudsters prey on individuals via dating or social media apps, gaining their trust and then seeking payment for claimed hardships.
- **Gold, gift card or cryptocurrency purchases:** In often complex scams, victims are convinced to purchase and hand over gold bars to criminals or to pay with gift cards, cryptocurrency (often by depositing cash at a crypto ATM) or other non-traditional methods that are hard to trace and nearly impossible to reverse.
- **Prizes/giveaways:** A fraudulent letter or email tells recipients they have won a prize—but need to pay “taxes” or other fees to claim it.
- **Check theft:** Physical checks are stolen from a mailbox or other vulnerable location, then doctored so they can be cashed. We see this issue frequently; if you must write a check, drop it off at the post office.

Worth Considering...

- Avoid clicking links or opening email attachments unless you were expecting the message and have verified the sender.
- By hovering over the sender's name in the "from" line, you can see their actual email address—a valuable clue in determining authenticity.
- Review your monthly statements closely. If you notice any unfamiliar transactions, contact your financial institution immediately.
- Update your apps and software on a timely basis to avoid leaving known vulnerabilities in place.
- Periodically inventory your digital footprint (social media, accounts with passwords, etc.) and close accounts you no longer need.
- Only share sensitive personal or financial information with secure, verified websites or trusted channels.
- Including "trusted contacts" on your financial accounts can enable providers to reach out to a friend or relative in the event of suspicious requests—particularly useful in protecting seniors.
- Avoid quizzes on social media if they require personal information.
- When shopping, tap—rather than insert or (the least safe option) swipe—your credit card to avoid the "skimming" of your card number.
- Don't use the same password on multiple accounts.
- If you suspect that you have been targeted by fraud, stop all communication with the perpetrator and contact your financial providers to secure your accounts. Other steps may be advisable (see "If Your Identity Is Stolen" on page 7).

know the word or you don't get into the car." That exact technique is now a defense against deepfakes. If someone claims to be a relative, but does not know the safe word, you should hang up. It may seem childish, but the technique works; AI can clone the voice, but won't know the secret word. Never text that word or write it down.

Be wary of deepfake video and audio. AI can now clone a voice or face convincingly, so seeing or hearing someone is no longer proof of who they are. Be suspicious of any call or video meeting that presses you to send money, share account details or keep a request secret, even if the person looks and sounds right. Don't count on spotting visual glitches; instead, hang up and call back on a number you trust, confirm information through a second channel and use your family safe word. Report any deepfake of you or a loved one to the platform involved and to the FBI at ic3.gov.

Assume your information is already out there. People don't like hearing this, but given the volume of breaches, you should assume that everything about you is effectively public. Many information-broker sites legally aggregate your addresses, phone numbers and relatives, but most offer removal. You can pay a service to take care of this or do it yourself, but the information may reappear online after the next breach. A better approach, in our view, is to spend your time securing what your information would be used to access—i.e., your accounts.

Freeze your credit. Widespread access to your information leads to another key point. In our view, everyone's credit should be frozen via the credit bureaus (see "Resources" on page 10). This is free, and makes it very hard for anyone to open new credit in your name without the required credentials. Should you need to do so, you can un-freeze your credit temporarily, and then re-freeze it when the process is over.

Lock your SIM card. Major carriers typically offer what may be called a number lock, port lock or SIM lock—all help prevent your phone number from being moved to another SIM or carrier without your approval. This takes just a few minutes and adds an important layer of protection to any account that sends verification codes by text.

Email is your most valuable account. It's where statements and notifications pile up, so it becomes the blueprint for everything you hold. It's also the recovery path for every other account. Stockpiled emails are a vulnerability, but probably not worth all the time and energy needed to empty them. Search out the few things that could actually hurt you—tax documents, statements, anything with a Social Security or full account number—and move them out of your inbox to a secure location on your computer or offline. Then use a separate email address for financial accounts. Be sure to give your email account the strongest login protection you have and assure that you have the ability to recover it should something go wrong.

Crime Stories

The following hypothetical examples are based on real-life incidents of fraud.

'Suspended' Account

Samuel received a text message that his account at an online retailer had been suspended. He clicked on the link provided to a seemingly authentic website, and called the listed phone number. Once on the line, he provided identifying information and was told that he needed to send cash to reinstate the account. The "operator" urged him to go to the bank and withdraw \$5,000, and to lie if asked about the purpose of the withdrawal. He became suspicious, hung up and contacted his financial providers to freeze his accounts.

Takeaway: Never click on links from unexpected texts or emails; be careful about "spoof" websites that may seek to access your information and defraud you. Reputable companies will never ask you to withdraw cash or mail it; they will certainly never instruct you to lie to a bank or anyone else. Such tactics are designed to keep you isolated and vulnerable.

Altered Wiring Instructions

Wiring instructions can be a focal point of theft, which is why financial institutions are generally very careful to make sure they are valid. Tony and Francine were each involved in a business transaction where emailed wiring instructions were intercepted and altered. Tony did not question the change and moved forward with a \$200,000 transfer, which was never recovered. Out of caution, Francine called the deal counterparty at an official number and found that the new instructions were fraudulent. She confirmed the proper instructions and completed the payment, later reporting the incident to the authorities.

Takeaway: In any transaction, always verify transfer details and then re-verify if they have been changed.

Payment in Gold Bars

A team of criminals exploited fear and secrecy to coerce Mary, a retiree, into turning over her life savings in the form of gold bars. The group impersonated U.S. marshals, claimed that Mary's identity had been compromised, and directed her to liquidate her savings and purchase gold as a supposed protective measure. She ultimately handed over gold bars valued at over \$100,000 and was further pressured to liquidate her retirement account for an additional \$400,000 before law enforcement intervened.

Takeaway: Never trust unexpected calls, texts or emails claiming your accounts are compromised or demanding secrecy; legitimate government agencies will never ask you to purchase gold or other precious metals, gift cards or cryptocurrency to safeguard your identity. Always go to official sources to verify these communications.

If Your Identity Is Stolen

Within the **first 24 hours**, it may be advisable to...

- Call your bank or brokerage at their published number and ask for a hold on outbound transfers
- Change your email password from a device you trust
- Freeze your credit via the three major credit reporting agencies (Experian, Equifax and TransUnion)
- Report the incident to the FBI (ic3.gov), which may be able to help trace funds, and the FTC (identitytheft.gov) for a recovery plan.

Speed is crucial; the odds of financial recovery drop sharply after the first day.

Understanding Your Authentication Options

Financial companies often suggest or require augmenting your password with multifactor authentication, which we think is a key security measure. Here are the various options you may encounter:

- **Code by text message.** A meaningful safeguard that can be made stronger by safe habits: Enter codes only on sites you reached yourself, not through a link in a message, and obtain a number lock from your mobile carrier (see “Lock Your SIM Card” on page 6) to help ensure only you receive the codes.
- **Authenticator app.** Generates rotating codes on your phone and is supported by many websites and apps.
- **Passkey.** Stored on your phone, in your browser or in a password manager, and unlocked with your face, fingerprint or PIN. Passkeys are designed to work only on the genuine website.
- **Physical security key.** A small device you plug in or tap, often used by those who want the highest level of protection. If you go this route, buy two so you have a spare.
- **Face or fingerprint recognition.** Usually unlocks your phone, a passkey or a password manager rather than serving as a separate step in the authentication process.
- **And one to reconsider: voice verification.** Because AI can now imitate voices from short recordings, consider asking your provider to turn it off.





Continued from page 6.

Device security still matters. Ransomware, where attackers take control of computers and require payment to unlock it, is a sizable industry; you can buy an attack on the dark web, with separate people taking on initial access, deployment and negotiating payment, each taking a fee. The process is largely offshore, in jurisdictions where U.S. law enforcement has limited reach. Although primarily focused on corporations, ransomware can affect individuals. So, keep your software current, leave the security tools enabled and maintain anti-phishing basics: Don't click on links in unexpected messages, don't open attachments you weren't expecting, don't reply to them and don't fill in forms on sites you reached by clicking on something.

Keep passwords strong. As we've noted before, passwords need to be complex and different for every account, particularly when it comes to email and financial accounts. And in our view, password managers (aggregating all your passwords in one secure application) are still worth the trouble: They now can store your passkeys, too, which can make them work across different device brands. At the same time, keep your recovery or backup codes in a safe physical location so you can avoid getting locked out of accounts.

Protect your family. This is an article in itself, but the key point is to address the unique vulnerabilities of family members. Aging parents may benefit from a trusted contact whom providers can consult in the event of concerning activity; duplicate statements, read-only access for family members, and in some cases, a power of attorney may be appropriate. Children should be educated about the dangers of online activity; and, in general, the family should make it a practice to engage in digital "hygiene," securing home networks, using effective passwords and limiting information provided on social media. Security should extend to vendors like an accountant or travel agency: Make sure that they engage in safe practices and that your communications of sensitive information are secure.

Conclusion: Building the Right Defenses

The task of securing your finances and identity involves compromises. It's more convenient to simply click on a link than call a financial institution first; it's easier to let your emails sit exposed than to cull them of sensitive information; and it's simpler to keep your credit active than to freeze it with multiple credit bureaus. But all of these steps have incremental benefits that help insulate you and your family from bad actors, as can maintaining healthy caution and good digital habits generally. Of course, there's always the chance that you will fall victim to a scam. In that case, we would argue that you should never be embarrassed or reluctant to share any issues with your trusted advisors or law enforcement. Such openness can help extricate you from difficult circumstances and hopefully foster more confidence as you navigate the more challenging "threatscape" that we encounter today.

Resources

ic3.gov. Report cyberfraud at this FBI website. Based on the information you provide, they can seek to trace and sometimes recover your funds.

identitytheft.gov. This FTC website generates a recovery plan to lock down and restore your finances, and provides an affidavit to protect you from creditor claims tied to the scam.

Annualcreditreport.com. Get free credit reports for the three major bureaus.

Experian.com, Equifax.com and TransUnion.com. Freeze your credit at the three major credit bureaus.

ChexSystems.com and EarlyWarning.com. Two lesser-known agencies that screen new bank accounts; we suggest freezing your credit with them as well.

National Elder Fraud Hotline: (833) 372-8311. Alerts the government to elder fraud; operators can help guide victims and their families through the recovery process.

Secure Our World (cisa.gov/secure-our-world). Plain-language guidance on protecting yourself online.

haveibeenpwned.com. Check whether your email has appeared in known data breaches.

Forward suspicious texts to 7726 to report them to your carrier.

The Growing Toll of Online Scams

\$20.9B

in reported U.S. losses,
up **26%** from \$16.6B
the prior year

1+ Million

complaints for the first time in
the report's 25-year history

191,561

Most-reported complaint type:
phishing and spoofing

\$7.7B

Victims 60 and older,
up **60%** in a single year
(37% of all losses)

Largest-Loss Crime Categories

\$8.6B

Investment fraud

\$3.0B

Business email
compromise

\$2.1B

Tech support scams

First year tracking
AI-related crime as its
own category: 22,364
complaints, just over

\$893M

This material is provided for informational and educational purposes only and nothing herein constitutes investment, legal, accounting or tax advice, or a recommendation to buy, sell or hold a security. This material is general in nature and is not directed to any category of investors and should not be regarded as individualized, a recommendation, investment advice or a suggestion to engage in or refrain from any investment-related course of action. Investment decisions and the appropriateness of this material should be made based on an investor's individual objectives and circumstances and in consultation with his or her advisors. This material is not intended as a formal research report and should not be relied upon as a basis for making an investment decision. The firm, its employees and advisory clients may hold positions within sectors discussed, including any companies specifically identified. Specific securities identified and described do not represent all of the securities purchased, sold or recommended for advisory clients. It should not be assumed that any investments in securities, companies, sectors or markets identified and described were or will be profitable. Neuberger, as well as its employees, does not provide tax or legal advice. You should consult your accountant, tax adviser and/or attorney for advice concerning your particular circumstances. Information is obtained from sources deemed reliable, but there is no representation or warranty as to its accuracy, completeness or reliability. All information is current as of the date of this material and is subject to change without notice. Any views or opinions expressed may not reflect those of the firm as a whole and Neuberger does not endorse any third-party views expressed. Third-party economic or market estimates discussed herein may or may not be realized and no opinion or representation is being given regarding such estimates. Neuberger products and services may not be available in all jurisdictions or to all client types. The use of tools cannot guarantee performance. Diversification does not guarantee profit or protect against loss in declining markets. As with any investment, there is the possibility of profit as well as the risk of loss. Investing entails risks, including possible loss of principal. Investments in hedge funds and private equity are speculative and involve a higher degree of risk than more traditional investments. Investments in hedge funds and private equity are intended for sophisticated investors only. Unless otherwise indicated, returns reflect reinvestment of dividends and distributions. Indexes are unmanaged and are not available for direct investment. This material may include estimates, outlooks, projections and other "forward-looking statements." Due to a variety of factors, actual events may differ significantly from those presented. Investing entails risks, including possible loss of principal. **Past performance is no guarantee of future results.**

Neuberger Berman Investment Advisers LLC is a registered investment adviser. The "Neuberger" name and logo are service marks of Neuberger Berman Group LLC.

NEUBERGER

1290 Avenue of the Americas
New York, NY 10104-0001
neuberger.com