Transamerica℠

Advanced Markets

Fraud alert

Your guide to protecting yourself in a changing world

Financial fraud is an issue that impacts all of us.

Knowledge is power

The good news, however, is that knowledge is power. The more we understand financial fraud and the common ways it's carried out, the easier it may be to avoid. This guide will provide an overview of several common scams, what to watch out for, and insights on how to protect yourself.

Fraud is common

Sadly, financial fraud is a big issue. The monetary estimates vary wildly but are thought to be in the billions.

Fraud can take a significant toll. Falling victim to fraud can have a severe emotional, and even physical, impact on victims. And with elder fraud, seniors often have no way to recoup the losses they suffer.

It's also on the rise

Data breaches happen more than we may ever know, exposing billions of records each year. Hackers target businesses – big and small – across a wide range of industries, from social media accounts to ride sharing services, and even healthcare companies. When you look at the millions of people impacted, it's no surprise that reports of identity theft are on the rise.

1 in 2

Prevalence of attacks

In 2021, one in two American internet users had their accounts breached[1]

[1] "The Latest 2023 Cyber Crime Statistics (Updated July 2023)," AAG, July 2023

1.9M

Apria Healthcare data breach, May 2023

1.9 million customers had personal data potentially exposed[2]

$10.3B

Online scams and losses rising

Over 800,000 cyber crime complaints in 2022 with losses of $10.3 billion[3]

Fraud often goes unreported

Even though fraud is so common, it may still be significantly underreported. So why wouldn't someone seek help? There are many possible reasons.

- **Embarrassment**
- **Dementia**
- **Fear of retaliation**
- **Doubt**
- **Involves a family member**
- **Don't know who to contact**

This means we need to be proactive in talking to people about fraud. Don't be afraid to ask questions. If you think someone you know might be a victim, let them know you can help.

[2] "Data Breaches That Have Happened in 2022 and 2023 So Far," Tech.co, June 2023
[3] "FBI Internet Crime Report," Internet Crime Complaint Center, July 2023

How to spot scams

When it comes to fraud, the more you know, the better off you are. Here are some common scams, as identified by the U.S. government.*

Common scams	Know the facts
Imposter scams (charity, debt, prize) Scammers pretend to be someone you trust, like a government employee or charity. The scam may relate to collecting a debt or winning a prize.	▪ Caller ID can be faked ▪ Don't provide any personal financial information ▪ You'll never win a contest you didn't enter
Imposter scams (grandparent) Scammers call claiming to be a grandchild in trouble or a police officer, lawyer, doctor, etc. calling on their behalf. They may urge you not to contact the parents and ask for money.	▪ Talk to your grandchildren about this scam ▪ Come up with an emergency code word ▪ Let them know you will always call their mom or dad
Mail fraud scams Any fraud that uses the U.S. Mail® is mail fraud. It could be relating to employment, telemarketing, veterans, finances, prizes, etc. and may originate online, over the phone, or by mail.	▪ See common mail fraud schemes at usps.com ▪ Don't share any financial information ▪ If you're a victim, file a complaint at 1-800-372-8347 or **uspis.gov/report**
Money transfer/mortgage fraud Be wary of people you don't know asking you to send money. Mortgage fraud targets homebuyers with complex schemes that appear legitimate.	▪ Never send money to someone you don't know ▪ Don't email financial information ▪ Never follow instructions contained in an email before verifying them with trusted individuals
Romance scams Criminals adopt a fake online identity to gain a victim's affection and trust. They establish a relationship as quickly as possible and make plans to meet that never happen.	▪ Be careful what you make public online ▪ Go slowly and ask lots of questions ▪ Be wary if an individual seems too perfect ▪ If you haven't met in person after a few months, you should be suspicious
Money mule scams A mule moves money that came from fraud victims. May be recruited through online job or social media posts, or by helping a love interest they met online or over the phone.	▪ Being a money mule can lead to jail time ▪ Don't send money or packages for people you don't know ▪ Don't open bank or crypto accounts for others ▪ Report scams at **reportfraud.ftc.gov**

* "What Are Some Common Types of Scams?" Consumer Financial Protection Bureau, April 2023

Technology:

How to protect yourself

There's no denying that modern technology brings countless benefits to today's world. On the flip side, it also creates certain vulnerabilities. The first step is to be aware of any potential issues, then decide what personal approach works best for you.

Smart phones

Privacy settings[4]

If you've ever wondered about the level of privacy you have on your cell phone or tablet, you're not alone.

- Before installing an app, know what it can access, review the permissions, and use official app stores.
- If you already have an app, review the permissions, don't sign in via social media, keep it updated, and delete if not using.

Location services[5]

This technology identifies the user's physical and geographical location, which is then used to provide information, entertainment, or security.

- It's based on access you allow on your phone and/or apps, and can be used to locate stores, get traffic updates, weather reports, ridesharing services, etc.
- The biggest disadvantage is the privacy concern in the event of a data breach. Some people prefer to limit app location services to when they're using the app or turn it off on their device.

[4] "How to Protect Your Privacy on Apps," Federal Trade Commission, accessed July 2023
[5] "Location-Based Services: Definition and Examples," Business News Daily, March 2023

Social Media

Despite the conspiracy theories, social media companies learn about you based on what you do in their apps and websites.[6]

- Virtual assistant apps like Siri or "Hey Google" are essentially verbal search engines that collect your data for marketing purposes. If you're concerned about privacy, you can disable them, and choose to limit permissions to apps that ask for microphone access.[7]
- TikTok, the largest social app with about 150 million users, is Chinese-owned and required by Chinese law to give the government access to collected data such as facial ID, voice prints, texts, locations, and photos. It can also collect your data if you click on a video linked to TikTok.[8]
- Use diligence when using social media marketplaces to buy goods. Be aware of scams and always be diligent on where you meet the other party to stay safe.
- Be careful of online dating apps and the possible scams. Common sense goes a long way, but never provide money to someone on a dating app.

Tip:

Don't put important personal information, such as your address or that you're away on vacation, on social media.

[6] "Here's How Facebook is Actually Listening to You," Komando.com, May 2022
[7] "Is My Phone Listening to Me? Yes, Here's Why and How to Stop It," Norton, June 2023
[8] "TikTok's Dark Side: Why It's More Than Just a Fun App and You Need to Remove It," Komando.com, March 2023

Artificial Intelligence

A new frontier[9]

According to IBM, at its simplest form, artificial intelligence (AI) is a field that combines computer science and robust datasets to enable problem-solving. Over the years, it's gone through many cycles of hype, but the release of OpenAI's ChatGPT seems to mark a turning point, particularly in natural language processing. But the generative models can also learn software code, molecules, natural images, and a variety of other data types.

The applications for this technology are growing every day, and we're just starting to explore the possibilities. Examples include speech recognition, customer service, computer vision, recommendation engines, and automated stock trading.

Deepfakes[10]

But as the hype around the use of AI in business takes off, conversations around ethics become critically important. AI-generated deepfakes are becoming more common. Deepfakes are a specific kind of synthetic media where a person in an image or video is swapped with another person's likeness. Or, it could be audio, with someone pretending to be someone you know.

Artificial intelligence is quickly getting better at mimicking reality, raising big questions over how to regulate it to avoid misuse like political propaganda or the creation of fake history. Countermeasures do exist, like software that can detect AI output, and AI tools that watermark the images or text they produce.

But there's no universal standard yet for identifying real or fake content. For now, the best way to move forward is to be skeptical, do some fact checking, and to do your best to determine if what you're seeing can be corroborated.

Cryptocurrency

Outpacing regulation

Cryptocurrency developments continue to outpace formal regulation. In 2022, the president issued an executive order on "Ensuring Responsible Development of Digital Assets." These new recommendations attempt to create a federal framework that addresses market integrity and consumer protection.[11]

[9] "What is Artificial Intelligence (AI)?" IBM.com, accessed September 2023
[10] "AI-Generated Deepfakes Are Moving Fast. Policymakers Can't Keep Up," NPR, April 2023
[11] "U.S. Treasury Encourages New Laws to Address Crypto Regulation Gaps," Reuters, October 2022

Crypto scams

In addition to the complex nature and lack of regulation in cryptocurrency, consumers should also be aware of common scams involving cryptocurrency. The first is simply fraudulent activity by bad actors, such as the case with FTX, a trading venture focused on digital assets that grew into a sprawling crypto empire, then collapsed because of improperly diverted assets by chief executive Sam Bankman-Fried.[12]

But the fact is, consumers tend to know very little when it comes to how digital currency works or how to keep their digital assets safe. And since cryptocurrency payments do not come with any legal protections or government assurances, crypto scams are especially attractive for thieves. There's also no centralized authority to flag suspicious crypto transactions, and all crypto transfers are irreversible. It's easy to see why the industry is ripe for fraud.[13]

Other cryptocurrency scams mirror some scams we've already discussed, but try to get cryptocurrency as the payment. According to the Federal Trade Commission (FTC), more than 46,000 people reported losing over $1 billion in crypto to various scams from January 2021 through June of 2022. And that figure only includes people who willingly shared the information with authorities.[13]

Tip:

As with other scams, just watch out for anything that seems too good to be true, "pay to play" job postings, promises of guaranteed returns, and unexpected communications regarding crypto.

[12] "The Crypto Fraud Case Against Sam Bankman-Fried and FTX," The Washington Post, September 2023
[13] "What Are The Most Popular Crypto Scams to Watch for in 2023," TIMEstamped, May 2023

Take action

Online

One way to protect your identity is to create online accounts for every financial or medical institution you work with. You may think that you're keeping yourself safe by not creating an online account, but you may be surprised to learn that the opposite is actually true. If you don't create an online account, someone else potentially can.

- ☐ Create online accounts and monitor them regularly.
- ☐ Use strong passwords, don't reuse them, and consider a password manager.
- ☐ Enable multi-factor authentication when available.
- ☐ Use auto-pay instead of sending a check in the mail.
- ☐ Don't overshare on social media (and tell your kids not to either).

Debit & credit cards

Not surprisingly, credit cards are a common target in financial abuse or exploitation. It could be a situation like phishing, where a thief steals credit card information. In other cases, a trusted person may get possession of a credit card and be tempted to use it for him or herself. Simple steps can reduce the risk of debit or credit card fraud.

- ☐ Don't use debit cards to make purchases and never give out your PIN. If compromised, the scammer has access to your bank account, similar to personal checks.
- ☐ Consider using a credit card with a low limit ($1,000 or $1,500) for day-to-day purchases like groceries, gas, or online purchases.
- ☐ Carefully review credit card statements for fraud. Watch out for things like magazine subscriptions and recurring charitable gifts, which could be a fraudulent income stream.

Electronic devices

Protect the physical devices that allow you to go online by taking the following action steps:

- ☐ Install anti-virus and anti-spyware software and keep them updated.
- ☐ Avoid phishing emails by not opening files or photos, clicking on links, or downloading programs sent by strangers. It could expose your system to a virus or spyware.
- ☐ Don't send personal information over your laptop or smartphone, especially on a public wireless network, like in a coffee shop or airport. They're not secure.
- ☐ Keep financial information on your devices only when necessary. Don't use an automatic login feature and log off when finished in case of theft. Safely dispose of data before replacing devices.
- ☐ Set up a security question, or a PIN with your cell phone provider. Otherwise, hackers can port your number and steal thousands of dollars from important accounts in a matter of days.

Identity theft

If you believe you've been the victim of identity theft, or if your personal information has been lost or exposed, identitytheft.gov (in Spanish at robodeidentidad.gov) is the government's free, one-stop resource for reporting and recovering from identity theft.

- ☐ Visit the site to get a personalized, interactive recovery plan.
- ☐ Follow the steps provided in your recovery plan, which may include prefilled letters, affidavits, and forms, follow-up reminders, advice for specific breaches, and plans for more than 30 types of ID theft.

Credit bureaus

Equifax, Experian, and Transunion collect information about where you live and work, how you pay your bills, whether you have been sued, arrested, or filed for bankruptcy. All of this information is combined in a credit report. The credit bureaus will sell your credit report to creditors, employers, insurers, and others. Those companies will then use the credit reports to make decisions about extending credit, jobs, and insurance policies to you.

- ☐ Find out how to obtain your credit report, make corrections, and more at **usa.gov/credit-reports**.
- ☐ Get information on fraud alerts and credit freezes at **consumer.ftc.gov**.

Offline

Even with so much of our lives being managed online these days, there are still risks associated "offline" as well. Mainly, you want to be careful with your mail and shred all documents with personally identifiable information before throwing them away or recycling them.

- ☐ Opt for e-delivery when possible to avoid sensitive material being mailed to you.
- ☐ Retrieve mail as quickly as possible to avoid theft.
- ☐ Place a hold on mail while on vacation.
- ☐ Have new checks mailed to your bank or other secure location.
- ☐ Shred all documents with personally identifiable information.

Social Security number

Your Social Security number is a coveted piece of information for criminals. Keep a close hold on it and ask questions before sharing it, including if you can use a different kind of identification. If someone asks you to share your number or your child's number, ask:

- ☐ Why it's needed
- ☐ How it will be used
- ☐ How it will be protected
- ☐ What happens if you don't share the number

If you think you're the target of a scam

There are a number of steps you can take to protect yourself.

First, be alert to financial fraud. Awareness is perhaps our most effective tool to fight scammers.

Second, if you suspect you've been defrauded, talk with someone you trust. Whether it's a spouse, adult child, attorney, tax advisor, or your financial professional, simply talking to someone about the situation can be helpful in determining whether fraud has occurred.

If you think it's a scam, you can call local law enforcement, your state attorney general, or the national credit bureau. Identifytheft.gov can also be a valuable resource to help create a recovery plan.

To learn more about Transamerica's Fraud Alert series and to get support materials:

Visit **transamerica.com**

Contact **your financial professional**

Transamerica. Live your best life.℠

3306919

Transamerica℠