Key Wealth

Key Wealth Institute

Preventing Fraud and Identity Theft

In this digital age, when more and more transactions are taking place on computers, mobile devices, and other technologies, criminals have focused on this trend to hone their craft of theft. According to the Federal Trade Commission (FTC), consumers lose billions of dollars to fraud each year[1]. In fact, identity theft was not the top complaint to the FTC in 2023, fraud was — with the top frauds being imposters, online shipping, prizes or sweepstakes, and investment scams. When looking at the amount of dollars lost, investment scams came in first. We will explore ways to identify signs of fraud and identity theft, how to protect yourself, and what you should do if you are a victim.

Top frauds

The largest fraud among the top five reported to the FTC was imposter scams, which typically start out with an unsolicited contact via phone, social media message, text, etc. A significant number involve the perpetrator pretending to be with a governmental agency, such as the Internal Revenue Service, Social Security Administration, or Medicare. Another top fraud involves online shopping, which can take several forms, such as discounted gift cards and e-mails from retailers you do not recognize. These emails have suspicious links that request personal information, which can be used for identity theft. Another online shopping fraud involves fake coupon site. The site will attempt to gather significant personal data to be used for identity theft before releasing a coupon code (which typically does not work).

The third top fraud involved prizes, sweepstakes, and lotteries. In these schemes, the fraudster reaches out via phone, text, or e-mail and tries to trick you into believing you won a prize of some sort. They indicate that they are from either a governmental agency or an organization you might be familiar with, like a charity or local fire department, and that you “won” a prize. If the fraudster says you need to pay some sort of fee (for taxes, processing, etc.); that paying a small fee increases your chances of winning (which would be illegal); or they request any bank/credit card information, it is likely a fraud.

The fourth largest fraud by number of reports filed with the FTC was investment fraud, with a median loss of over $7,700 per incident. Investment fraud can come in several varieties, such as receiving investment information via social media, crypto investment scams, high-yield investment programs, pre-IPO investment scams, and pump-and-dump schemes. While there are a lot of different types, there are some common techniques to help you avoid investment fraud. These include watching for returns that are "guaranteed" (who are they guaranteed by?); investments that sound too good to be true (they probably are); opportunities offered by an unknown salesperson; and unsolicited offers. It's important to research firms that offer you investment opportunities; you can check the Securities and Exchange Commission (SEC) or Financial Industry Regulatory Authority (FINRA) databases for information. Additionally, you should verify the identity of the source of the opportunity and never make investment decisions based solely on information from social media platforms or apps.

Business and job opportunity fraud is the fifth largest fraud category reported. These involve schemes that offer help starting up a business or fake job listings or employment services. Some of these opportunities are just pyramid schemes, in which you only make money if you recruit new participants, or a trick to obtain your personal information. To avoid being a victim, research the job opportunity with the company directly and be wary of providing personal information to unknown entities. Also, don't cash/deposit a check that is forwarded to you to "get you started." In this type of fraud, the new employer asks you to return the unused portion of the check, and the check will bounce; you will be out the unspent funds you sent back to the employer.

Identity theft

Some of the frauds listed above have as their goal to get as much of your personal information as they can so they can steal your identity. Different types of identity theft include financial identity theft, medical identity theft, online identity theft, account takeover fraud, and mortgage fraud. By stealing your name, address, credit card, bank account numbers, and/or medical insurance account numbers, a criminal can obtain credit in your name, file a fraudulent tax return and obtain your tax refund, open accounts in your name such as utilities or mobile plans, and use your health insurance to get medical care. Identity theft happens in many ways, from as simple as theft of a purse or wallet that contain personal information to retrieving financial documents from your garbage. More sophisticated techniques include getting your personal information from your computer or mobile device when you are using a public Wi-Fi, installing "skimmers" at checkouts to get information from the card you used, and using information from your social media accounts (be careful of what you post).

Any type of identity theft is a frighting and frustrating experience that can not only impact you financially, but also negatively impact your credit rating.

Warning signs that you are a victim of identity theft

Unlike most crimes, it may take a while to realize that you are a victim of identity theft, so it is helpful to know some of the warning signs. The most common involve unexplained financial activity, including receiving bills for items you did not purchase or calls from debt collectors for accounts you did not open, or other unauthorized transactions. Sometimes the fraudster will give your card a trial run for minor amounts, such as a few dollars. If you see one of these minor unexplained transactions, contact the credit card company immediately so they can block the transaction and even issue you a new card. Another sign of fraud is that you stop receiving or are missing mail (especially from financial institutions, including credit card companies) or are receiving unexpected/unusual correspondence from your health care provider or the Internal Revenue Service (or your state taxing authority). Other warning signs include the denial of loan applications, significant changes to your credit score, and losing access to your accounts.

Protect from identity theft

With the variety of fraud we reviewed above, protecting yourself from identity theft is not a one-time endeavor but an ongoing process in which you need to be constantly vigilant. One of the steps to protect yourself is requesting and monitoring your credit report on a regular basis. The three major credit reporting agencies are required to provide, upon request, a free credit report at least once per year. It can be requested by visiting annualcreditreport.com and should be reviewed on a regular basis for anything unusual or unexpected. You should also audit and change your passwords regularly and consider using a password manager, which both remembers and changes your passwords automatically. Using multifactor authentication (which is a way to confirm your identity when you sign into your online accounts) especially for your financial accounts is strongly suggested, along with shredding all financial and other documents that contain any personal information. Additionally, financial documents should be kept in a secure location (such as a locked file cabinet).

Enrolling in an identity theft protection plan is something to consider. They charge a small monthly fee, but they notify you of any suspicious activity, may reimburse you for any losses, and can help you through the process of restoration should you become a victim of identity theft. It's also a smart idea to use a different e-mail account for online shopping, so you can keep your banking and other financial logins separate from social media and shopping accounts. Finally, if asked (either in person or via phone, e-mail, text, or any social media outlet) for any personal information, take a step back and ask yourself why they need it. Is this something that seems too good to be true, and are you about to have a fraud perpetrated on yourself?

If you are a victim of identity theft, there are several immediate steps you should take:

- Go to Federal Trade Commission online at IdentityTheft.gov (or call 1-877-438-4338) to report it. The FTC has specific information on all the steps you should take in an easy-to-follow format.
- Contact all three major credit reporting agencies to place fraud alerts and a credit freeze on your accounts.
- Reach out to the fraud department at all the financial institutions you do business with (including all credit card issuers).
- File a report with your local police department and make sure you get a copy of the report, since you may need it for some of the steps you will need to take to repair the damage.

For more information, please contact your advisor.

The Key Wealth Institute is a team of highly experienced professionals representing various disciplines within wealth management who are dedicated to delivering timely insights and practical advice. From strategies designed to better manage your wealth, to guidance to help you better understand the world impacting your wealth, Key Wealth Institute provides proactive insights needed to navigate your financial journey.

Key Wealth

[1]Federal Trade Commission. (February 2024). Consumer Sentinel Network: Data Book 2023. ftc.gov/data

The Key Wealth Institute is comprised of financial professionals representing KeyBank National Association (KeyBank) and certain affiliates, such as Key Investment Services LLC (KIS) and KeyCorp Insurance Agency USA Inc. (KIA).

Any opinions, projections, or recommendations contained herein are subject to change without notice, are those of the individual author(s), and may not necessarily represent the views of KeyBank or any of its subsidiaries or affiliates.

This material presented is for informational purposes only and is not intended to be an offer, recommendation, or solicitation to purchase or sell any security or product or to employ a specific investment or tax planning strategy.

KeyBank, nor its subsidiaries or affiliates, represent, warrant or guarantee that this material is accurate, complete or suitable for any purpose or any investor and it should not be used as a basis for investment or tax planning decisions. It is not to be relied upon or used in substitution for the exercise of independent judgment. It should not be construed as individual tax, legal or financial advice.

The summaries, prices, quotes and/or statistics contained herein have been obtained from sources believed to be reliable but are not necessarily complete and cannot be guaranteed. They are provided for informational purposes only and are not intended to replace any confirmations or statements. Past performance does not guarantee future results.

Investment products, brokerage and investment advisory services are offered through KIS, member FINRA/SIPC and SEC-registered investment advisor. Insurance products are offered through KIA. Insurance products offered through KIA are underwritten by and the obligation of insurance companies that are not affiliated with KeyBank.

Non-deposit products are:

NOT FDIC INSURED • NOT BANK GUARANTEED • MAY LOSE VALUE • NOT A DEPOSIT • NOT INSURED BY ANY FEDERAL OR STATE GOVERNMENT AGENCY