6 MERIDIAN

How to Protect Your Financial Information

Consumer financial fraud has risen sharply in recent years, with losses reaching billions and continuing to grow year over year as part of a sustained multi-year trend.[1] Protecting your identity, financial well-being and privacy in the face of these threats is of utmost importance. The following seven steps can go a long way toward this effort.

01 | STAY EDUCATED ON RECENT TRENDS IN FRAUD TACTICS AND SCAMS

- Follow reputable news sources that report on fraud and cybersecurity issues. These sources can provide valuable insights into emerging scams and trends.
- Subscribe to newsletters or blogs from organizations that specialize in fraud prevention, such as government agencies, financial institutions, or cybersecurity companies. These often provide updates, tips, and best practices for recognizing fraud.
- Before taking action, thoroughly research any requests or offers you receive. Evaluate their legitimacy, consider whether they align with your expectations, and verify the credibility of the source. Be skeptical of unsolicited communications and requests for personal information.

02 | KEEP YOUR CHECKBOOKS, CREDIT CARDS, BANK STATEMENTS, AND IDS IN A SECURE PLACE

These items contain sensitive information that, if obtained by unauthorized individuals, could lead to fraud and financial harm. To protect yourself, consider the following:

- Be mindful of your surroundings when handling sensitive information in public. Ensure others cannot easily see your account numbers, PINs, or passwords. Shield your information when making transactions or accessing accounts in crowded or unfamiliar environments.
- Securely dispose of documents containing personal information. Use a shredder to destroy outdated identification cards, old debit cards, bank statements, or other unnecessary paperwork.
- Keep your account numbers, credit card numbers, and ID information private. Avoid sharing this information whenever possible.

03 | REGULARLY REVIEW YOUR FINANCIAL INFORMATION FOR SUSPICIOUS ACTIVITY OR ANY UNAUTHORIZED CHARGES

- Set up transaction alerts or notifications from your financial institutions to receive real-time updates on account activity.
- Review each transaction carefully to ensure you recognize and have authorized it.
- Monitor your credit reports by obtaining free annual reports from credit bureaus or using credit monitoring services, and report any unusual activity.
- Use online banking on your desktop or mobile device to check your accounts frequently.

04 | BE CAUTIOUS OF UNSOLICITED OFFERS, AND SKEPTICAL OF REQUESTS FOR MONEY OR PERSONAL INFORMATION

Trust your instincts. If something does not feel right about a phone call, email, or advertisement, it may not be legitimate. Confirm who you are sending money to, ensure the transaction makes sense, and verify the reason for the request.

05 | KEEP YOUR COMPUTER'S SECURITY SOFTWARE UP TO DATE, AND USE A SECURE WIFI NETWORK

Keeping your computer up to date will help protect you against malware, enhance online safety, mitigate remote attacks and increase vulnerability patching (updates that address security vulnerabilities). To do this, we suggest you:

- Enable automatic updates for your operating system and security software, or regularly check for updates manually.
- Install updates for all software applications regularly.
- Avoid using public Wi-Fi networks for sensitive activities such as banking online or accessing personal accounts.
- Consider using a virtual private network (VPN) for an added layer of security when accessing the internet.

06 | USE STRONG PASSWORDS AND MULTI-FACTOR AUTHENTICATION

- Create long, complex passwords using a combination of numbers, symbols, and letters.
- Use unique passwords for each account and update them regularly.

07 | BE CAUTIOUS OF TARGETED TELEPHONE CALLS

- Avoid sharing banking or personal information over the phone, and do not feel pressured to act immediately.
- Be wary of the question, "Can you hear me?" which may be used to record a "yes" response for fraudulent purposes.
- Remember that law enforcement agencies and the IRS typically do not initiate contact by phone.

CONCLUSION

By following these recommendations, you can strengthen your awareness of fraud tactics and better protect yourself. Staying informed and using available resources can help you recognize and respond to potential threats.

As these practices highlight, cybercriminals may be persistent, but their methods can often be mitigated through ongoing awareness and caution. We also continue to evolve our defenses to help safeguard your data as we communicate with you.

FOOTNOTES

[1]Consumer Sentinel Network reports. (n.d.). Federal Trade Commission. Retrieved April 7, 2026, from https://www.ftc.gov/enforcement/consumer-sentinel-network/reports1

DISCLOSURES