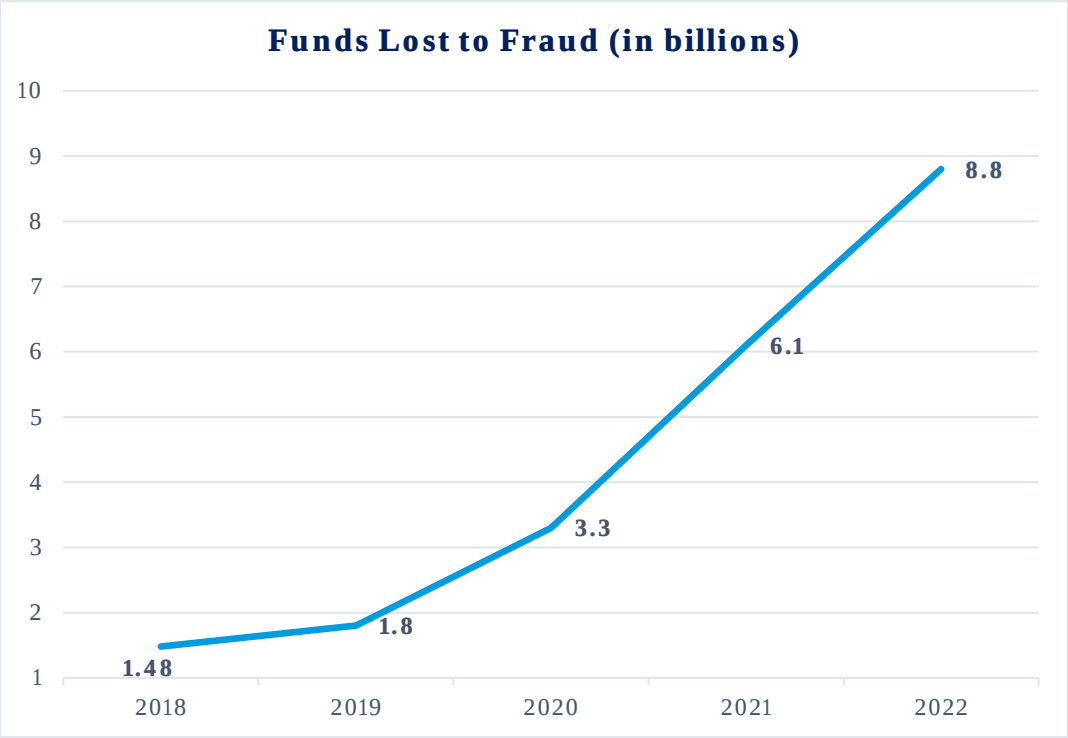
hield Your Wealth:
Seven Steps to Better Protect your Financial Information

June 2023

In 2022, consumer financial fraud reached alarming levels. Reported losses totaled nearly $8.8 billion,[1] which represented an increase of more than 30% over the previous year. Unfortunately, this frightening increase in fraud has been a consistent trend over the last five years.



Source: Federal Trade Commission. As of February 2018 – February 2023.

The rise of social media and advancing technology have contributed to an increase in scams targeting all demographics. Protecting your identity, financial well-being and privacy is of utmost importance in the face of these threats. The following seven steps can help provide significant protection in addition to valuable peace of mind.

1. Stay educated on recent trends in fraud tactics and scams.

[1]*Federal Trade Commission. As of February 23, 2023.* https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-datashowconsumersreportedlosingnearly88billionscams2022#:~:text=Newly%20released%20Federal%20Trade%20Commission%20data%20shows%20that,than%20%243.8%20billion%E2%80%94than%20any%20other%20category%20in%20202

- Follow reputable news sources that report on fraud and cyber security issues. These sources provide valuable insights into emerging scams and fraud trends.
- Subscribe to newsletters or blogs from organizations that specialize in fraud prevention, such as government agencies, financial institutions, or cybersecurity companies. These newsletters often provide updates, tips and best practices for recognizing fraud.
- Before taking any actions, research the request or offer thoroughly. Evaluate its legitimacy, consider if it aligns with your expectations, and verify the credibility of the source. Always be skeptical of unsolicited communications and requests for personal information.

2. **Keep your checkbooks, credit cards, bank statements and IDs in a secure, safe place**.
   These items contain sensitive information which, if obtained by unauthorized individuals, could lead to various forms of fraud and financial harm. To protect yourself, consider the following measures:
   - Be mindful of your surroundings when handling sensitive information in public. Ensure that others cannot easily see your account numbers, PINS or passwords while you are using them. Shield your information when making transactions or accessing your accounts in crowded or unfamiliar environments.
   - Dispose of any documentation that contains personal information securely. Use a shredder to destroy outdated identification cards, old debit cards, bank statements or any other paperwork that is no longer needed.
   - Keep your account numbers, credit card numbers and ID information to yourself. Avoid sharing account numbers with others. The more confidential you keep such information, the less likely it is that it will fall into the wrong hands.

3. **Regularly review your financial information for suspicious activity or any unauthorized charges**.
   - Set-up transaction alerts or notifications from your financial institutions to your mobile device to receive real-time updates on account activity.
   - Scrutinize each transaction and verify that you recognize and have authorized them.
   - Keep track of your credit reports by obtaining free annual reports from credit bureaus or using credit monitoring services to stay informed about any unusual activities.
   - Utilize online banking on both your desktop and your mobile device to monitor your accounts frequently.

4. **Be cautious of unsolicited offers and be skeptical of requests for money or your personal information.**
   Always trust your instincts. If something does not feel right about a phone call, email, or advertisement, it may not be legitimate and thus warrants further caution. Be sure you know who you are sending money to, that the transaction makes sense and that the reason you are sending the money makes sense.

5. **Be sure to keep your computer up to date on security software and use a secure Wi-Fi 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 online banking or accessing personal accounts.
- Consider using a virtual private network (VPN) for an added layer of security when accessing the internet.

6. Use strong passwords and multi-factor authentication.

- Use a combination of numbers, symbols and letters to form a long, complex password.
- Use unique passwords for each online login and regularly change all passwords.

7. Be cautious of targeted telephone calls:

- Avoid divulging any banking or personal information to a caller over the phone, and do not give in to pressure to take immediate action.
- Beware of the question "Can you hear me?" which may lead to the recording of you responding "yes" to authorize unwanted charges, etc.
- Remember that law enforcement agencies and the IRS will not call you.

By following these recommendations, we believe you can enhance your awareness of fraud tactics and scams, enabling you to protect yourself more effectively. Keeping up with the latest information and resources ensures you are well-equipped to recognize and respond to potential threats.

For more information, please contact any of the professionals at Plaza Advisory Group, Inc.