HOW TO PROTECT YOUR PERSONAL INFORMATION

Individuals are constantly reminded about how important it is to protect their personal information. If your information is exposed, a fraudster can either take over your identity completely or create a synthetic identity with some of your information. In either scenario, the fraudster can negatively impact your credit score with a long road to restitution. But how does one safeguard this information?

The following measures are potential ways you can help protect your information and monitor financial activity:

PASSWORD AND ACCOUNT MANAGEMENT

Protecting your accounts is fundamental to your security, as these accounts typically have additional sensitive information that can be exploited.

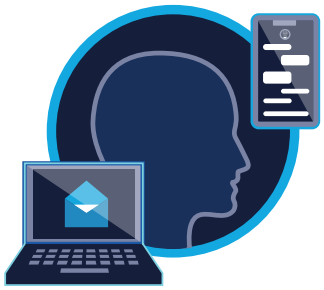
- **Create strong passwords, ensuring they are unique and not easily guessed.**
  Do not include these commonly used sources in your password: name of a loved one (including pets), birthdays or anniversaries.

- **Use a different password for different accounts or websites.**
  If you use the same password for multiple accounts, it puts all those accounts at risk should a data breach occur. For example, fraudsters use a tactic called "credential stuffing," in which login credentials that are stolen or exposed from one service are used to attempt to break into other accounts or services.

- **Create or select unique security questions, whose answers cannot be guessed or accessed via public records or social media.**
  Information that used to be considered private or hard to find – such as your mother's maiden name, your father's middle name and the street you grew up on – can now easily be obtained on the internet. Additionally, anything you share on social media becomes insights for someone trying to crack your password or security questions. Be mindful of what you share on social media and how that could affect the privacy of the information you choose for your security questions and answers.

HOW TO PROTECT YOUR PERSONAL INFORMATION

- **Where possible, enable multi-factor authentication (MFA) on your accounts.**
  Enabling MFA helps ensure that the user is granted access only after presenting two pieces of evidence (or factors) to an authentication mechanism. The three factors used are: something you know, something you have and something you are. Using MFA helps protect accounts from being accessed by an unauthorized party who may have been able to obtain one of those pieces (e.g., login or password). For example, in addition to your login credentials, you also may have to enter a code that was sent to your mobile device.



DILIGENCE IN COMMUNICATION

Fraudsters target individuals through various forms of communication. They often use emotions or fear to trick you into acting. If an outreach seems to play to your emotions or emphasizes an urgency to act, it is likely that someone is trying to get your information. Being aware of this overall strategy can help keep you from unknowingly giving fraudsters your valuable information. Fraudsters can communicate in some of the following ways: emails, text messages, phone calls and social media.

Here are some general tips for ensuring diligence in your communications:

- **If it seems suspect, trust your instincts** and question whether the outreach is legitimate.

- **Do not click on links** in emails or text messages from unknown senders. This could initiate malware on your device, likely exposing your personal information as a result of the malware.

- **Do not provide or confirm any of your personal information** when contacted by another party. Legitimate parties typically already have this information, so asking for the information is a red flag. If you believe the inquiry may be legitimate and are a customer of that organization, a good practice is to contact them using information on the company website.

HOW TO PROTECT YOUR PERSONAL INFORMATION

PHYSICAL PROTECTION

While we are living in a digital world, we also must consider physical security to safeguard our personal information.

- **Be aware of your surroundings.** Fraudsters often pick up information by simply being near you physically. When using a mobile device, be cognizant of who is around and use a privacy screen, if possible. Also, when having conversations – either in person or via phone – ensure you're not providing confidential information to someone listening nearby.

- **Lock up any sensitive information.** For sensitive documents you keep in hard copy form, store them in a safe location, ideally in a locked cabinet or drawer or safety deposit box.

- **Securely destroy unneeded documents.** Shred and destroy any physical documents containing personal or financial information that you no longer need.

MONITORING AND PROTECTING YOUR CREDIT

Even if you put these safeguards into place, it's important to actively monitor the safety of your accounts. One way of doing this is to vigorously monitor and manage your credit reports, reviewing them for any surprising or suspicious activity.

- **Monitoring your credit:**
  - ***Requesting your credit report:*** Federal law gives you the right to a free copy of your credit report every 12 months. The three national credit bureaus have a centralized service for ordering the three reports in one place. To obtain your credit report from all three bureaus (Equifax, Experian, and TransUnion):
    - Visit: annualcreditreport.com; or
    - Call: 1-877-322-8228.

    Other circumstances may allow more frequent requests at no charge. Visit the ***Federal Trade Commission's (FTC) Free Credit Report*** webpage for more information.

HOW TO PROTECT YOUR PERSONAL INFORMATION

- ***Reviewing your credit reports:*** Review the reports for account openings or other activity that does not seem in line with your account openings, payment history, etc.

- **Safeguarding your accounts:**

  Fraudsters target individuals who may not actively be using their credit accounts, knowing their fraudulent activity will likely go unnoticed for a while. If you anticipate that you won't be opening new accounts for a duration of time, you can freeze your credit temporarily. By doing so, you are preventing fraudsters from opening new lines of credit under your name or using some of your personal information to create a synthetic identity to open new accounts. Visit these websites to begin the process to request a credit freeze or security freeze from each of the credit bureaus:

  - ***Equifax***
  - ***Experian***
  - ***TransUnion***

TAKE ACTION

By leveraging these practices, you can help safeguard your personal information, reducing the risk of it being compromised and used for fraudulent purposes.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.