# Proactive Measures to Protect Your Identity

FIDUCIARY™ TRUST

## Information Security Insights

*Identity theft and fraud are rampant. Since 2017 there have been almost 13,000 data breaches exposing nearly 6.5 billion personal records, according to the Identity Theft Resource Center. With so many records exposed, there has been a corresponding increase in fraud, with the Federal Trade Commission (FTC) receiving fraud reports from 2.6 million consumers in 2023, representing more than $10 billion in losses. With more than 1 million of these reports related to identity theft, it is estimated that approximately 22% of Americans are subjected to identity theft each year, especially since not all cases are reported to the FTC. Given the continued importance of identity protection, we are sharing this updated and complete version of our article on this topic, which was initially published in 2020.*

Although you may not be able to control whether your personal information is exposed in a data breach, there are actions you can take to protect yourself against fraud-related identity theft:

1. **Obtain and Carefully Review Your Credit Reports:** Under federal law, each person is entitled to one free copy of their credit report annually from each of the three major credit reporting bureaus, which include Equifax, Experian, and TransUnion. This can easily be done by visiting www.annualcreditreport.com/index.action, the only website sanctioned by federal law to obtain these free reports. In addition, each of the three agencies allows anyone to obtain a free weekly credit report, which can also be obtained from each agency if you sign up for a free account with that agency.

### Learn More:

For more insights or information on Fiduciary Trust visit:

www.FidTrustCo.com

### or contact:

Sid Queler
queler@fiduciary-trust.com
617-292-6799

**Once you obtain one or more of your credit reports, you should review each of them carefully**

Once you obtain one or more of your credit reports, you should review each of them carefully. Reports can be quite lengthy, but any detail that is incorrect could complicate things for you later or be a sign that there has been an unauthorized attempt to utilize your credit.

Items to pay particular attention to include: your personal information, such as your name, current and prior addresses, phone numbers, and date of birth; credit accounts such as credit cards, car loans, and mortgages; and credit inquiries. The credit inquiries indicate what entities have accessed your credit history for some reason. Entities that you have a credit relationship with, such as a credit card issuer, will access your report periodically to verify that you are still a good credit risk. Beyond that, inquiries should be monitored, as they are usually the first step in establishing new credit, which includes actions like opening a new credit card, obtaining a mortgage, or renting an apartment.

If anything appears suspicious, you should reach out directly to the entity that made the inquiry to see if an account has been established or if there was an attempt to establish an account with your credentials. If you see a problem with your personal information, such as your address or phone numbers, you should contact the credit bureau to correct it.

Please note that knowing your Fair Isaac Corporation (FICO) score is not the same as reviewing your detailed credit report. Your credit report includes your credit history and critical personal information. Your FICO score is a numeric gauge that helps you and creditors assess how good of a credit risk you may be. Your FICO score is based on various elements including your utilization of available credit, payment history, types of credit utilized, new credit inquiries, and length of credit history.

2. **Set up Your My Social Security Account:** If you have not done so, you should establish your My Social Security account by visiting www.ssa.gov/myaccount/. Obtaining your credit report will help in answering the security questions required by the Social Security Administration (SSA). These questions are designed to ensure that it is you attempting to set up your account in order to prevent fraud. If you answer any questions incorrectly, you will be locked out for 24 hours.

   There are many reasons to set up a My Social Security account, including the ability to easily verify your earnings history, to protect your Social Security benefits, and to establish direct deposit of benefits. The most significant reason, however, is to stop someone else from establishing the account and potentially claiming benefits in your name or redirecting benefits to which you may be entitled. If your identity with the SSA is ever compromised you may not be able to set up an account, which is why anyone over the age of 18 should set up their account now. If you find that you have been the victim of Social Security fraud, you should report it at www.ssa.gov/scam/.

3. **Guard Your Social Security Number (SSN):** Never provide your SSN unless you trust the other party and you are sure that they require it for a valid reason. The fewer databases that contain your SSN, or even your driver's license number, the less likely your identity is to be compromised. Many forms, including

medical questionnaires, ask for your SSN but may not have a legally valid reason for requiring it. For example, if your medical provider has your insurance information, they do not have a right to your SSN. Parties that do have either a legal right to or a need to have your SSN include those who must verify your identity under the federal Consumer Identification Program or who are required to report to the IRS. Among those with a legitimate right to require your SSN are employers, banks, investment advisors, insurance companies, and lenders, as well as the credit bureaus and many government agencies, including the IRS and the Department of Motor Vehicles. To protect yourself, do not carry your Social Security card in your wallet.

4. **Freeze Your Credit:** You should seriously consider freezing your credit. Freezing your credit blocks potential new creditors from accessing your credit reports, thus making it unlikely that new credit would be granted on your credentials without your knowledge. After you freeze your credit, you need to "thaw" it, or unfreeze it temporarily, if you decide to apply for new credit, such as a new mortgage or credit card, or if you want to rent an apartment.

   There is no cost to either freezing or unfreezing your credit and it can be done very easily, but you must do it separately with each bureau. Unfreezing your credit allows the potential creditor to have access to your credit information. It is recommended that when you unfreeze your credit file, you instruct it to automatically refreeze after a chosen interval of time, such as a few days or a week. Remember to maintain a list of your usernames and passwords/access codes that you set up when you froze your credit. Freezing your credit does not affect your ability to utilize your current credit cards or stop current creditors, or a limited group of others, from accessing your credit information.

   The act of freezing your credit is easily done online by visiting each of the three main credit bureaus' websites. Once the credit bureau verifies it is you, you can freeze your credit with that bureau. Each bureau will follow up with a letter confirming your decision and may provide you with a PIN number, if you did not create one at the time of freezing. It is important to retain any login information and PIN numbers so that you can easily unfreeze your credit later.

   In addition to the three major credit bureaus, there is a fourth, lesser-known bureau, Innovis, where you may also want to consider freezing your credit. Although less critical than the big three, there is no significant downside to also freezing your credit with the fourth bureau. The links to the credit bureau websites to freeze your credit are:

   Equifax: www.equifax.com/personal/credit-report-services/credit-freeze/
   Experian: www.experian.com/freeze/center.html
   Transunion: www.transunion.com/credit-freeze
   Innovis: www.innovis.com/personal/securityFreeze

   Even if your credit is frozen, you need to remain vigilant about periodically reviewing your credit reports because problems can still arise. In addition to your own credit, you should consider freezing the credit of your minor child who is under the age of 16 and assisting disabled or elderly family members to accomplish the same.

**To protect yourself, do not carry your Social Security card in your wallet**

Learn More:

Access our full library of insights at fidtrustco.com/insights

**Remain vigilant and as you review your mail, emails, text messages, and phone solicitations**

*Minor Children:* A minor child's identity is among the most lucrative for identity thieves since if a child's identity is compromised it may not be discovered for many years, until they apply for credit as an adult. A parent or guardian can freeze their child's credit by contacting each of the above agencies. This process is usually not immediate, as the agency will need to review the information you provide, often by mail, to make sure you have the right to request the freeze for the minor.

- Equifax: assets.equifax.com/assets/personal/Minor_Freeze_Request_Form.pdf
- Experian: www.experian.com/help/minor-request.html
- Transunion: www.transunion.com/credit-freeze/credit-freeze-faq#freeze-other-minor-0

*Military Active-Duty Alert:* Deployed members of the military are a particularly attractive target for identity thieves. It is recommended that service members place an Active-Duty Alert on their credit file by contacting one of the three major credit bureaus. The first bureau will inform the other bureaus of the alert. The alert is valid for one year, but can be renewed, and will remove the person from prescreened credit card offers for two years unless he or she requests to be put back on the list.

5. **Consider Credit Monitoring Services:** Some choose to sign up for credit monitoring services to help provide timely notice of any suspicious activity. There are several services available to do this, either through the credit bureaus, credit card companies, or other companies dedicated to this service. Some services are free, while others are not. If you choose to sign up for a service, make sure it is reputable and will provide you with whatever types of monitoring you deem important.

Please remember that signing up for a credit monitoring service is not a substitute for remaining diligent about protecting your identity and reviewing your credit reports. If you are notified that your information was compromised during a security breach and are offered free credit monitoring, there is little downside to signing up for the free period.

6. **Be Cautious and Watch for Phishing or Other Scams:** Remain vigilant as you review your mail, emails, text messages, and phone solicitations. You should examine your mail carefully for indications that your identity may have been compromised, not click on links or open attachments that are not from trusted sources, or provide your personal, banking, or credit card information unless you are completely sure it is prudent to do so.

7. **Be Leery of Unsolicited Mail:**

   *Read, but Verify, and Take Appropriate Action:* If you receive a letter or email from the state indicating you have filed for unemployment benefits when you have not, you will want to take action immediately. The same goes for correspondence from collection agencies on accounts that are not yours or letters from the IRS or Social Security Administration (SSA). Instead of calling back any phone numbers or clicking on any links that may appear in the correspondence, go online to independently verify contact information before you reach out.

   Be careful not to reveal your personal information until you are sure you are dealing with a legitimate party. Remember that neither the IRS nor the SSA will call you unless you are in a dialogue with them already, and if they do call, they will not ask you for your full Social Security number, bank account information, or credit card number. If you receive a letter saying a credit application you did not submit has been denied, this is a red flag of potential problems.

   *Preapproved Credit Card Offers:* If you are not interested in receiving preapproved credit card offers, you can opt-out for either five years or permanently. Call 888-567-8688 or visit www.optoutprescreen.com/ to begin the process.

8. **Review Your Credit Card, Bank, and Investment Statements:** Whether you receive these by mail or online, you should review them carefully for unauthorized activity. If your credit card provides it, consider signing up for notifications for "card not present transactions" and other signs of fraudulent activity, so that you can respond quickly in the event of a breach.

9. **Shred Sensitive Information:** "Dumpster diving" is one of the ways that thieves can obtain information about you, so be sure to shred any documents that include sensitive information.

10. **Delete Questionable Emails and Texts:** Along with not clicking on links or attachments in questionable correspondence, it is prudent to immediately delete them and even empty your trash folder.

11. **Let Phone Calls from Unknown Parties Go to Voicemail:** If it is important and legitimate, they will leave a message.

**Be careful not to reveal your personal information until you are sure you are dealing with a legitimate party**

Author

Jody R. King, JD, CPA, AEP®, RLP®, CDFA®, Vice President & Director of Wealth Planning

**12. Use Unique Passwords Online:** Periodically update your unique, hard-to-guess passwords for each of your online accounts, including email, credit, bank, and all other accounts. To keep your detailed login information secure, either use a password-keeper application or maintain a paper-based documentation system. Utilize multi-factor authentication whenever it is available. If you do request and utilize an email allowing you to reset a password, immediately delete it and empty your email trash folder after using it to reset your password. Doing so can help protect you if an unscrupulous party has gained access to your email.

If you are concerned that your identity may have been compromised, please review *Key Steps to Take If Your Identity Has Been Compromised*.

It is always easier to protect and maintain your identity than it is to recover from identity theft. Taking proactive steps today to secure your identity, including reviewing your credit reports and freezing your credit, can ultimately save you significant time and stress. If your identity is compromised, quick and decisive action can help to limit the damage.

## Learn More:

For more insights or information on Fiduciary Trust visit:

www.FidTrustCo.com

## or contact:

Sid Queler
queler@fiduciary-trust.com
617-292-6799