Ways to Protect Yourself Better from Identity Theft

Presented by LifeTime Asset Management, LLC

As we learned from the Equifax breach in 2017, anyone can fall victim to identity theft through no fault of their own. Although mastering every potential identity theft scenario isn't feasible, learning more about the identity theft tools and services available to you—and how best to initiate a recovery plan if you become a victim—is well worth your time.

A great starting point for victims of identity theft is identitytheft.gov. By following the site's simple prompts, you can select your identity theft situation, access guidance and resources specific to you, and file identity theft reports with the FTC.

Here, we review four types of remediation resources and services available to the public, from the most lightweight to the most robust, focusing on the benefits and risks of each. Keep in mind that these tools may be used concurrently.

Credit Monitoring

This type of service keeps track of your credit file, aiming to catch any changes or suspicious activity, so you don't have to check on it yourself. Credit-monitoring services can send alerts (most often by email or text message) anytime someone performs a hard credit inquiry or opens a new line of credit. If anything looks fishy, you can report the unauthorized activity to the company holding that account, as well as to the major credit bureaus. At this stage, some incidents may be remediated.

Benefits

- This service often comes free of charge after major breaches (e.g., Equifax, Anthem) in which social security numbers have been exposed.
- Credit monitoring doesn't restrict your access to your credit file.

Risks

- Credit monitoring is reactive and notifies users only after unauthorized activity has occurred.
- Requires entrusting your social security number to another company.
- Monitors credit only, not other accounts.

Fraud Alerts

This tool is a cautionary note that you can place on your credit report. It tells credit lenders or service providers that you may have been a victim of identity theft and compels them to verify any changes to your credit before making them. For example, if you apply for a credit card while you have a fraud alert in place, the credit card company may call you to verify that you—and not an identity thief—submitted the application. Verification usually happens over the phone, but current law does not specify a standard means of verification.

There are two types of fraud alerts: *initial* fraud alerts (which stay in place for one year) and *extended* fraud alerts (which extend that time to seven years). To implement an extended fraud alert, you're required to file an identity theft report first with the Federal Trade Commission (FTC).

Benefits

- Fraud alerts are completely free.
- They are easy to set up. You can submit a request to one major credit bureau, and that bureau will notify the other two bureaus.
- Fraud alerts don't restrict your access to your credit file.

Risks

- The verification process isn't clearly defined by law.
- Verification could cause delays in credit changes.
- This measure doesn't protect existing accounts.

Credit Freezes

As the name indicates, this tool *freezes* credit files so that no one—including the individual who placed the freeze—can open a new line of credit. Before opening a new line of credit, you would first have to unfreeze your credit file with a personal identification number (PIN) provided by the credit bureau. This is the most restrictive tool you can administer on your own, but using it has consequences.

Benefits

- A freeze is the most effective preventive measure; with it in place, no changes can be made to the credit file without the PIN.
- As of September 2018, credit freezes are free in all 50 states.

Risks

- The application process requires a separate submission to each of the three credit bureaus.
- A freeze restricts access to your own credit. You must unfreeze it to allow changes. (Changes may be permitted for specific companies at specific times.)
- It doesn't restrict access to your existing accounts; fraudulent activity can still occur in those.

Identity Theft Protection Services

Identity theft protection services bundle a suite of helpful tools and resources into one package. The better services offer real-time credit monitoring at all three major bureaus, customized account alerts (for more than just credit), and a 24/7 call center.

Benefits

- These services combine the benefits of other tools (e.g., credit monitoring and alerts).
- With 24/7 support (where available), a service can help guide you through the appropriate steps to mitigate the situation at any time.
- Some services can monitor accounts outside of credit files.

Risks

- Requires entrusting your social security number to another company.
- These services can be costly.
- Quality may vary, so before subscribing to any service, be sure to perform due diligence.
- Most vendors won't help with identity theft that took place before you subscribed to their services.

Preventing a part two. After remediation, maintaining healthy account hygiene can help prevent unauthorized activity in the future. Here are some tips:

- **Change account passwords** for all accounts that may have been compromised.
- **Ensure your passwords are unique** for each account. That way, if one account is compromised, the attackers can't potentially use its credentials to access your other accounts.
- **Enable multifactor authentication** wherever possible. It asks users to provide more than one form of identification to log in to their accounts. For example, in addition to entering a password or PIN, you would be prompted to access something you have, such as a smartphone or hardware.
- **Review mail-forwarding rules on your account**, particularly if you suspect your email has been hacked, and delete any messages you don't recognize. In many cases, attackers add forwarding rules such that, when accounts send or receive certain e-mails, the e-mails are forwarded to another address—even after you've regained access and changed your passwords.

If you have any questions about the information provided here, please feel free to call or email my office.

These hyperlinks are being provided as a courtesy and are for informational purposes only. We make no representation regarding the completeness or accuracy of information provided at these websites.

LifeTime Asset Management, LLC
801 Corporate Center Drive | Suite 110 | Raleigh, NC 27607
919.845.5315 | 919.845.5346 fax | www.lifetimeasset.com