MORGAN & MORGAN

In the aftermath of a data breach, it is very important for anyone whose personal information that was publicly exposed to take steps to protect their credit and finances. While not exhaustive, the following list provides a number of actions that consumers should consider taking to protect themselves.

1. **Put a fraud alert on your credit reports.**

   A fraud alert flags your credit report and notifies lenders and creditors that they should take extra steps to verify your identity before extending credit. To place a fraud alert on all three of your credit reports, you only need to contact one of the three credit reporting agencies (Experian, Equifax, or TransUnion). When you place the initial alert, the agency will automatically notify the other two for you.

   When you place a fraud alert on your credit reports, you're entitled to a free copy of your credit report from each of the three agencies. Be sure to obtain them. If you find fraudulent items on your credit report(s), the simplest way to begin the dispute process is to click the dispute button while viewing your credit report online. Some items must be disputed in writing and with supporting documentation. Hard inquiries cannot be disputed, but may give you a clue as to where a thief has applied for credit in your name.

   Another option is to place a security freeze on each of your credit reports. A freeze prevents creditors (except those with whom you already do business) from accessing your credit report(s) at all. Most new applications will automatically be declined because without access to your file, the creditor will have no way to evaluate your credit. With a security freeze in place, you will need to take extra steps if you wish to apply for new credit. Each agency has a procedure for temporarily "thawing" your file in order to allow a legitimate application to be processed. Unlike a fraud alert, however, you'll need to contact each credit reporting agency individually to place a freeze on your files. See more information about credit freezes here:

   - **Experian**: https://www.experian.com/freeze/center.html
   - **Equifax**: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
   - **TransUnion**: https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

2. **Sign up for a credit monitoring service.**

   There are a number of companies that offer credit monitoring services, and consumers should select the one which fits their individual needs. The following link provides a list of a number of them:

   http://www.reviews.com/identity-theft-protection-services/

3. **Review your credit reports for suspicious activity, such as accounts that you do not recognize.**

   Request copies from all three major reporting agencies, and look for any accounts you may not recognize. By law, you're entitled to at least one free credit report from each agency each year. While plenty of websites and creditors promise free credit reports, the official site to request them is www.AnnualCreditReport.com.

4. **Contact the Federal Trade Commission (FTC).**

   Report the incident directly to the Federal Trade Commission by submitting an Identity Theft Report. You can file your report online at: (https://www.ftc.gov/faq/consumer-protection/submit-consumer-complaint-ftc) or (https://www.identitytheft.gov), by phone (toll-free): 1-877-ID THEFT (877-438-4338); TDD (toll-free): 1-866-653-4261, or by mail — 600 Pennsylvania Ave., Washington DC 20580.

   The FTC will provide you with information about what to do next, depending on what type of fraud was (or may have been) committed.

5. **File a police report.**

   In addition to filing a report with the federal government, you should also contact your local police department. This step isn't as much about getting the police to investigate the crime as it is about creating a paper trail to show you were proactively addressing the problem. Although the police may not be able to do anything if your identity was stolen by criminals online and overseas, your report could help them track down someone who is stealing information locally.

6. **Protect your Social Security number.**

   If your social security number was or may have been compromised, contact the Social Security Administration (800-269-0271) and the Internal Revenue Service (800-829-0433).

   It's important to talk to the Social Security Administration and the Internal Revenue Service if you have reason to believe your Social Security number has been compromised, even if you don't yet see any evidence of financial fraud. A thief could be planning to swipe your tax refund, or to obtain employment or health care in your name.

7. **Contact the Post Office.**

   If you have reason to believe the identity thief may have submitted a fraudulent change-of-address to the post office or has used the U.S. mail to commit the fraud against you, contact the Postal Inspection Service, which is the law enforcement and security branch of the post office. You may report any suspicious activity in this regard online at https://postalinspectors.uspis.gov/.

8. **Scan credit card and bank statements for unauthorized charges.**

   Pull up your accounts and scan old statements for charges you don't recognize. Don't forget to review dormant or infrequently used accounts as well. If you find unknown charges, call the financial institutions to alert them of the problem and request the account be locked or closed.

9. **Implement preventive measures going forward.**

   Although some cases of identity theft are unavoidable, there are ways to make yourself less likely to be a victim. These include the following:

   - Creating strong passwords and regularly changing them.
   - Shredding documents with personal information when disposing them.
   - Keeping personal information such as your address and phone number off social media sites, as well as any details you use for online security questions like your mother's maiden name.
   - Do not carry your Social Security card in your wallet.

10. **Use caution when reviewing suspicious emails.**

    Clicking unknown links in emails is another way to make yourself an easy target for identity thieves. Clicking a link sent to you by an identity thief could result in you inadvertently downloading malware or Keylogger software that thieves use to mine your computer for personal information.

This list is not meant to be exhaustive and there may be other protective measures that you should consider taking based upon your personal situation and finances. There are also other sources of information that you may want to consult, including but not limited to:

Federal Trade Commission: https://www.ftc.gov/data-breach-resources
The Federal Bureau of Investigation: https://www.fbi.gov/investigate/cyber
Internal Revenue Service: https://www.irs.gov/identity-theft-fraud-scams/data-breach-information-for-taxpayers