PROTECTING YOURSELF FROM IDENTITY THEFT

AVOIDING IDENTITY THEFT

1. Do not disclose your full nine-digit Social Security number unless absolutely necessary, and never use it as an identifier or password. Question those who ask for it.
2. Avoid paper billing by requesting secure electronic statements instead. If you require hard copies, you can print and store them safely without risking mail theft.
3. Lock your mailbox.
4. Shred documents containing personal information (name, account numbers, social security number, birth date) before throwing them away.
5. Configure your computer and/or smartphone to require a password for use, and set another password for sensitive files. Use unique passwords that include a combination of letters, numbers, and symbols. Do not use your birth date, a close relative's birth date, or a combination of letters and numbers on **Splashdata's annual list of the most stolen passwords**.
6. Avoid using the same password for different accounts, and change your passwords once or twice per year.
7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, and smartphones.
8. Don't disclose information commonly used to verify your identity on social networking sites, such as date of birth, city of birth, mother's maiden name, name of high school, etc. If you do, don't use that information to verify your identity.
9. Avoid making purchases, paying bills, or sending sensitive information over unsecured WiFi networks (at airports, coffee shops, or hotels).
10. Disable Bluetooth connections on devices when not in use.
11. Watch out for "phishing" scams. Phishing is when identity thieves request personal information by pretending to be a legitimate entity, such as a bank or the IRS. Ignore unsolicited requests for personal information by email or over the phone, and only contact entities by means you know to be authentic. Do not contact an entity by clicking a link sent as part of an email requesting personal information, because phishers often link to authentic-looking, fake webpages. You can also call the phone number on the back of a card previously issued to you, or call the phone number on an old statement from that issuer.
12. Fight "skimmers." Do not give your debit card to a server or anyone who could have a hand-held skimming device out of sight. When using an ATM, look for suspicious cameras and holes, and touch to confirm that extra parts have not been installed. Always cover your hand while hand typing a PIN, and avoid using ATMs in secluded locations.

13. When accessing financial information on your smartphone, only use apps authorized by your bank or published by reputable app makers. Apps that show thousands of downloads are probably safe.

DETECTING IDENTITY THEFT

14. Check your monthly statements for unauthorized charges.
15. Sign up to receive email and/or text notifications of account activity and changes to account information.
16. Get your free annual credit report. Every 12 months, you are entitled to receive one free credit report from each of the three main credit reporting agencies. Instead of requesting three at the same time, request one credit report from one of the agencies every four months. Verify that the information is correct, and an account has not been opened without your knowledge. Free credit reports are available online at **AnnualCreditReport.com** or by calling 1-877-322-8228.

WHAT TO DO WHEN YOU DETECT IDENTITY THEFT

Step 1: Notify your financial institutions.

If you discover that your wallet, checkbook, credit card or other sensitive information has been lost or stolen, immediately notify the issuing bank, credit card issuer, or relevant institution to close all existing accounts.

Step 2: Get an Identify Theft Affidavit.

If you suspect identity theft, report it to the Federal Trade Commission using the **online complaint form** or by calling 1-877-ID-THEFT. When making the report, you will be given an option to receive an Identity Theft Affidavit. This document, together with the police report, will be critical to minimizing the damage.

Step 3: File a police report.

If you believe you are a victim of identity theft, file a report with your local police department. When you make the report, bring a copy of the Identity Theft Affidavit. The police report will be important for insurance purposes. Keep copies of the police report and Identity Theft Affidavit.

Step 4: Contact the three major credit reporting companies and place a fraud alert and security freeze on your accounts.

An important next step is to place a fraud alert and a security freeze on your credit report. Placing a fraud alert tells businesses checking your credit rating that there may be fraud involved in the account. The fraud alert

must be renewed after 90 days, and it entitles you to receive one free credit report from each of the main agencies. The security freeze stops anyone from seeing your credit report without your permission. Alerts and freezes can be placed by contacting the toll-free fraud number of any of the three consumer reporting companies noted below. Initiating a credit freeze does not impact your credit score.

- TransUnion: 1-800-680-7289; **www.transunion.com**; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- Equifax: 1-800-525-6285; **www.equifax.com**; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); **www.experian.com; P.O. Box 9554, Allen, TX 75013**

Step 5: If your social security number was stolen, contact the Social Security Administration.

File a report and access resources at **www.idtheft.gov**. You can also call 1-800-772-1213.

MORE IDENTITY THEFT RESOURCES

- Consumer Federation of America (**idtheftinfo.org**)
- Identity Theft Assistance Center (**www.identitytheftassistance.org**)
- Identity Theft Council (**www.identitytheftcouncil.org**)
- Identity Theft Resource Center (**www.idtheftcenter.org**)
- Federal Trade Commission: Identity Theft (**www.consumer.ftc.gov/features/feature-0014-identity-theft**)
- Privacy Rights Clearinghouse (**www.privacyrights.org**)
- More Government Resources (**www.idtheft.gov**)