How to Detect and Protect Yourself from Identity Theft

1) Keep your Social Security Number Safe

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.
Also, shred documents containing personal information (name, account numbers, social security number, birth date) before throwing them away.

2) Keep Yourself Safe with Electronic Billing Options

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. Also, lock your mailbox if it's lockable.

3) Keep yourself Safe on Your Computer and Cellphone

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**.

Also, avoid using the same password for different accounts, and change your passwords once or twice per year. It is also a good idea to install and update antivirus, anti-malware, and security programs on all computers, tablets, and smartphones.

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.

4) Keep Yourself Safe on the Internet

Avoid using credit or debit cards or conducting online banking transactions or making purchases, paying bills, or sending sensitive information over unsecured WiFi networks (e.g., any network without a password log-in, such as on trains, at airports, coffee shops, or hotels).

Watch out for "phishing" and other "social engineering" 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.

5) Keep Yourself Safe from "Skimmers"
Fight "skimmers." Do not give your debit card to a restaurant 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 (loose or slightly different colors) have not been installed over the card reader. Always cover your hand while hand typing a PIN, and avoid using ATMs in secluded locations.

6) Freeze Your Credit Reports
Place security, or credit freezes, on your credit report. Our separate **"security freeze" tips** explain how to guarantee peace of mind against new account identity theft by freezing your credit reports, then thawing them only when you are in the credit markets. A creditor will deny credit to an imposter who applies for credit using the name and Social Security Number of a consumer who has placed a freeze.

7) Use Free Annual Credit Reports
Instead of paying for over-priced subscription credit monitoring, use your free annual credit reports by law as your own credit monitoring service. Every 12 months, federal law gives you the right to receive one free credit report from each of the three main consumer reporting agencies, Equifax, Experian and TransUnion. Instead of requesting three at the same time, request one credit report from one of the bureaus 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. Seven states – Colorado, Georgia, Maine, Massachusetts, Maryland, New Jersey and Vermont also provide an additional free report by state law, available by contacting each bureau directly.

8) Types of Identity Theft: Existing Account Fraud
Federal law recognizes two sorts of identity theft—existing account fraud and new account (account takeover) identity theft.

Victims of data breaches where only their account numbers were taken are well-protected by law, although victims of lost debit card numbers may face bounced checks and cash flow problems until the bank replaces their funds. The Electronic Funds Transfer Act (EFTA) provides for no liability if you notify the financial institution within 60 days if only your debit card numbers are stolen. However, if you actually lose a debit card or other device that can access your bank account, your liability could be up to $500 if you fail to notify the bank within 2 days of finding out about the loss and could increase even higher if you fail to notify the bank within 60 days. Under the separate

Truth In Lending Act, credit card customers are always well protected by law, never facing liability of greater than $50 for fraudulent use of a card.

9) Types of Identity Theft: New Account Identity Theft

A thief who obtains your Social Security Number may attempt to open new accounts in your name. This form of identity theft is difficult to clear up. A thief who obtains your email address may contact you in a phishing scam to try and trick you into providing your SSN and birth date, which are the keys to new account identity theft. Thieves apply for credit with your name, your SSN and their own address. The creditor then obtains a credit report and issues credit to the thief.

10) Be Wary of New Types of Identity Theft

Note that online tax preparers and the IRS itself have been hacked, resulting in tax refund fraud. Health insurance data breaches may result in medical services theft. A federal agency, the Office of Personnel Management (OPM), has recently been breached. Detailed security clearance dossiers that were taken provide thieves with the opportunity to commit new account identity theft and could subject victims to reputational risk and emotional harms, since information on possible marital affairs, drug and alcohol abuse treatment, previous arrests even without convictions, may have been taken.

11) What To Do When You Detect New Account 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.

12) What To Do When You Detect New Account Identity Theft (continued)

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 on your accounts. If you haven't already, **it's time to place a security freeze**.

13) Place a Fraud Alert on Your Credit Report

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

14) Take Action for Stolen Social Security Numbers

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.

15) 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**)