IDENTITY THEFT

Security Breaches

Our economy generates an enormous amount of data. Most users of that information are from honest businesses - getting and giving legitimate information. Despite the benefits of the information age, some consumers may want to limit the amount of personal information they share.

When your personal information is sold or gets into circulation, it poses two threats: you will receive more unwanted solicitations – and/or you could become the victim of "identity theft" such as someone opening an account using your name. Guard your personal information – especially your credit cards, bank accounts, and Social Security Number (SSN).

Every day you share personal information about yourself with others. It's so routine that you may not even realize you're doing it. You may write a check at the grocery store, charge tickets to the ball game, rent a car, mail your tax returns, schedule a doctor's appointment or apply for a credit card. Each transaction requires you to share personal information such as:

- Bank and credit card account numbers
- Income
- Social Security Number (SSN)
- Name, address, and phone numbers

There are unscrupulous individuals, like identity thieves, who want your information to commit fraud.

Identity theft occurs when someone uses your personal identifying information, like your name, SSN, or bank or credit card number, without your permission, to commit fraud or other crimes. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.

Identity theft is serious. It is viewed by many consumer privacy groups as the fastest growing, white collar crime in the nation. Federal Trade Commission (FTC) statistics indicate that nearly 5% of the adult U.S. populations have been a victim of identity thefts, with losses totaling more than $5 billion. It can be devastating when someone uses another individual's

SOUTH DAKOTA OFFICE OF ATTORNEY GENERAL
CONSUMER PROTECTION
1302 E Hwy 14 Ste 3 • Pierre SD 57501 consumerhelp@state.sd.us
1-800-300-1986

personal identifying information to commit fraud. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for educations, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

Keeping Your Personal Information Secure Offline

- **Lock It Up.** Your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.
- **Limit what you carry.** When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you are going to use your card at the doctor's office.
- **Why do they need it?** Before you share information at your workplace, a business, your child's school, or a doctor's office, ask: why they need it, how they will safeguard it, and the consequences of not sharing.
- **Shred it.** Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.
- **Destroy it.** Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.
- **Grab the mail.** Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a vacation hold on your mail.
- **Ordering checks.** When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

Keeping Your Personal Information Secure Online

- **Be Alert to Impersonators.** Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.
- **Safely Dispose of Personal Information.** Before you dispose of a computer or electronic device, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received,

voicemails, messages sent and received, organizer folders, web search history, and photos.

- **Encrypt Your Data.** Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.
- **Keep Passwords Private.** Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.
- **Don't Overshare on Social Networking Sites.** If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Protecting Your Social Security Number (SSN)

Keep a close hold on your Social Security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's, ask why they need it, how it will be used, how they will protect it, and what happens if you don't share the number?

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

What To Do If You're Identity Is Stolen

- Cancel all credit cards
- Request a letter from the bank or credit institution confirming that a fraud has been committed against you and that you are not responsible for the ensuing debt.
- Close any of your accounts that have been compromised.
- File a police report with your local police or sheriff's office. You can also file a police report in the jurisdiction where the theft occurred and obtain a copy to show creditors. When filing the report please ask the person taking the report about the National Crime Information Center (NCIC) Identity Theft report.
- Call the three (3) national credit reporting agencies (Equifax, Experian, and TransUnion) to place a fraud alert on your name and social security number. Refer to the *Reference Guide* section for contact information.
- Take notes and keep a record of conversations and make copies of correspondences. Retain this information indefinitely.

- Contact the Federal Trade Commission Identity Theft Hot Line at 877-ID-THEFT (877-438-4338) to file a complaint.
- Contact the Department of Motor Vehicles to ensure that no unauthorized license(s) have been issued in your name.
- After all related matters are corrected, request new credit reports to confirm that fact.

Top Identity Theft Crimes:

- Credit Card Fraud
- Cellular Phone Fraud
- Check Fraud
- Loan Fraud
- Government Benefits Fraud

Identity theft happens when someone steals your personal information and uses it without your permission. It's a serious crime that can wreak havoc with your finances, credit history, and reputation — and can take time, money, and patience to resolve. The average victim spends approximately 175 hours (more than four (4) forty (40) hour work weeks) to repair identity theft damage.

Keeping Your Devices Secure

- **Use Security Software.** Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Installing these types of programs will help protect against intrusions and infections that can compromise your computer files and passwords. These programs install security patches for your operating system and other software programs.
- **Avoid Phishing Emails.** Don't open files, click on links, or download programs sent by strangers**.** Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.
- **Be Wise About Wi-Fi.** Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.
- **Lock Up Your Laptop.** Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.
- **Read Privacy Policies.** Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

SECURITY BREACHES

Have you received a letter informing you that your personal information may have gotten into the wrong hands? It is increasingly common for companies, educational institutions, and government agencies (whether or not their state has a breach notice law) to notify individuals when computer files containing personal information have been hacked, stolen, or lost. If the file includes your SSN, financial account numbers, driver's license numbers, or data that would be useful to identity thieves, there are steps you can take to reduce your risk of fraud.

What should you do if you receive a letter telling you that your personal information has been compromised?
First, don't panic. A security breach does not necessarily mean that you will become a victim of identity theft.

1. Figure out what type of breach has occurred. Has a breach occurred with your *existing* financial account? Has your SSN been compromised, with the chance that *new accounts* can be established by an imposter? Has your driver's license number been compromised, or another government-issued ID document?

- **Existing accounts.** If the breach involved your *existing* credit or debit card account, you will want to monitor your monthly account statements very carefully. Contact the creditor if your statement does not arrive on time. A missing bill could mean that an identity thief has changed your address. Check statements for transactions you did not make. Dispute those fraudulent charges directly with the credit or debit card company. The company will likely cancel the account and give you a new card and account number. You will not be responsible for the fraudulent charges if you properly dispute them. It's very important to report the fraudulent transactions immediately. In some situations, the financial company will not wait for evidence of fraud. It will instead cancel the existing account and issue a new account number right away.
- **The potential for new accounts to be opened**. If the breach involved disclosure of your SSN, a fraudster could use that information to open *new accounts* in your name. You will not immediately know of the new accounts because criminals usually use an address other than your own for the account. Since you will not be receiving the monthly account statements, you are likely to be unaware of the account(s). That is why it is so important to place a fraud alert with the three credit reporting agencies immediately when you learn that your SSN has been compromised, and then to monitor your credit reports on an ongoing basis. Other evidence of new account fraud include receiving credit cards in the mail that you did not apply for, being denied credit when you know you've had a good credit score, and being contacted by debt collectors for payments that you do not owe.
- **ID Documents.** Nearly all the security breaches reported to date have potentially involved financial accounts. But if you are notified of a breach involving your driver's license or another government document, contact the agency that issued the document and find out what it recommends in such situations. You might be instructed to cancel the document and obtain a replacement, or the agency might instead "flag" your file to prevent an imposter from getting a license in your name.

2. For security breach situations involving your Social Security Number (SSN) — in other words, breaches in which there is an opportunity for new accounts to be opened in your name you should consider taking the following actions:

- **Notify the credit reporting agencies and establish a fraud alert.** Immediately call the fraud department of one of the three credit reporting agencies — Experian, Equifax, or TransUnion. As soon as the agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.
- **Order your credit reports.** If you are a victim of identity theft, you will see evidence of it on your credit report. Surveys have found that the sooner individuals learn of the identity theft, the more quickly they can clean up their credit reports and regain their financial health.
- **Examine your credit reports carefully**. When you receive your credit reports, look for signs of fraud such as credit accounts that are not yours. Check if there are numerous inquiries on your credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on your credit report for each of those attempts. Usually identity thieves do not succeed in opening all of the accounts that they apply for, only some. Multiple inquiries that you yourself have not generated are a sign of potential fraud. Also, check that your SSN, address(es), phone number(s), and employment information are correct.
- **If your credit report indicates you are a victim of identity theft, you will want to immediately take steps to remove the fraudulent accounts**. If you are a victim you may contact the Federal Trade Commission or the SD Office of Attorney General website for step-by-step information on what you should do.
- **Contact Social Security Administration at 1-800-772-1213.** Do this to verify earnings reported to your social security number and to request a copy of your Social Security Statement.
- **Continue to monitor your credit reports.** Be aware that these measures may not entirely stop new fraudulent accounts from being opened by an imposter. Credit issuers do not always pay attention to fraud alerts. Once you have received the first free copy of your credit report, follow up in a few months and order another.
- **Consider a security freeze.** The three credit reporting agencies — Equifax, Experian, and TransUnion, offer security freezes nationwide. Read on for further information.