Consumer Alert: How to Protect Your Identity from Being Stolen

Despite your best efforts to manage the flow of your personal information, identity thieves may try a variety of methods to gain access to your data. For instance, they may get information from your discarded mail, stealing your wallet/purse, stealing information they find in your home or through your computer/email, or stealing information/records from the workplace. Criminals can then open credit cards with your name, take your existing financial accounts, forge drivers' licenses and other government documents, among other things. The DMA has provided a number of steps you can take today to minimize your risk of being a victim of identity theft.

1. Use Unique or Unpredictable Passwords:

Place unidentifiable passwords on all of your accounts -- your credit card, bank and phone accounts. Avoid using easily available information such as your mother's maiden name, your birth date, the last four digits of your Social Security Number (SSN) or your phone number, or a series of consecutive numbers.

2. Secure Personal Information:

In your home

- Take precautions if you have roommates, employ outside help, or are having repair work done on/in your home.
- Lock personal information in a filing cabinet.
- Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox, and promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, call the US Postal Service at 800.275.8777 or go online: https://dunsapp.usps.gov/HoldMail.jsp to request a hold.
- Tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

- When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.

On the phone/Internet

- Don't give out personal information unless you've initiated contact or are sure you know who you're dealing with.
- Be cautious when responding to promotional offers. Identity thieves may create phony promotional offers to get you to give them your personal information.
- Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their SSN, mother's maiden name, account numbers, and other personal information. Before you share any such information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line. Or call customer service using the number listed on your account statement or in the telephone book.

In your mail

- Deposit mail in the US Postal Service collection boxes or directly at your local post office.
- Don't leave mail in your mailbox overnight or on weekends.

In your wallet

- Don't carry your SSN card; leave it in a secure place. Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your state uses your SSN as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your policy number.
- Carry only the identification information and the credit and debit cards that you'll actually need when you go out.
- Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

On your computer

- Update virus protection software and patches for your operating system and other software programs regularly.

- Do not open files sent to you by strangers, or click on hyperlinks or download programs from people you don't know. Be careful about using file-sharing programs. Opening a file could expose your system to a computer virus or a program known as "spyware," which could capture your passwords or any other information as you type it into your keyboard.

- Use a firewall program to stop uninvited access to your computer. Without it, hackers can take over your computer, access the personal information stored on it, and use it to commit crimes

- Use a secure browser - software that encrypts or scrambles information you send over the Internet - to guard your online transactions. Be sure your browser has the most up-to-date encryption capabilities by using the latest version available from the manufacturer. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

- Try not to store financial information on your laptop unless absolutely necessary. If you do, use a strong password a combination of letters (upper and lower case), numbers and symbols.

- Before you dispose of a computer, delete all the personal information it had stored. Use a "wipe" utility program to overwrite the entire hard drive. Deleting files using the keyboard or mouse commands or reformatting your hard drive may not be enough because the files may stay on the computer's hard drive, where they may be retrieved easily.

- Look for website's privacy policies. They should answer questions about maintaining accuracy, access, security, and control of personal information collected by the site, how the information will be used, and whether it will be provided to third parties. If you don't see a privacy policy – or if you can't understand it – consider doing business elsewhere.

3. Educate Yourself on Security Procedures Outside of the Home:

- Ask about information security procedures in your workplace or at businesses, doctors' offices or other institutions that collect your personal identifying information.

- Find out who has access to your personal information, and verify that it is handled securely.

- Ask about disposal procedures for your records.
- Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

4. Check Your Credit Report:

- One of the most important ways to protect yourself against Identity Theft is to check your credit report status often
- Under federal law (the Fair and Accurate Credit Transactions Act – FACTA), you are entitled to one free credit report per year: contact www.annualcreditreport.com.
- If you believe you are a victim of identity theft, you can request that a fraud alert be placed on your credit report to signal this to prospective users of that report

Other Resources:

- **Federal Trade Commission:** Take Charge: Fighting Back Against Identity Theft http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm
- **US Postal Inspection Service:** Tips for Avoiding ID Theft and How to Report ID Theft https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/mailtheft/IdentityTheft.aspx
- **US Department of Justice:** What are Identity Theft and Identity Fraud? http://www.justice.gov/criminal/fraud/websites/idtheft.html
- **Federal Deposit Insurance Company (FDIC):** Identity Theft & Fraud http://www.fdic.gov/consumers/theft/index.html