IDENTITY THEFT — BE AWARE, PREPARE, AND TAKE CARE

According to the U.S. Secret Service, the revenue from trafficking financial data has surpassed that of trafficking drugs. The Bureau of Justice Statistics (BJS) released a survey in December 2013 reporting that an estimated 16.6 million people (7% of all Americans age 16 or older) were victims of identity theft in 2012. Those victims reported a total of $24.7 billion in direct and indirect losses. There are an estimated 27,000 new victims every day — 1 out of 10 children and 1 out of 6 adults annually, as reported by the Federal Trade Commission.

If you use an ATM, debit or credit card, have a bank account, own a cell phone, own a home, have a mortgage, have health insurance, have applied for loans or other credit, have ever seen a doctor or use the internet — you are at risk for identity theft.

Identity theft can cause you to be denied college financial aid, auto loans, apartment rentals, home purchases, credit cards, life insurance, employment based on false medical history or criminal record, etc. It can also cause you to lose your driver's license and can ruin your career.

COMMON TYPES OF IDENTITY THEFT:

- Identity thieves use your personal information to clean out your bank accounts, cash in your investments, apply for credit cards or loans, buy thousands of dollars of merchandise, etc.
- Identity thieves use your Social Security number to get a tax refund or a job.
- Identity thieves use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider or get other care.
- Identity thieves provide your personal information to law enforcement when caught breaking the law.
- Identity thieves use your personal information to live as you — popular for illegal immigrants or criminals hiding from the law.

HOW IDENTITY THIEVES GET YOUR INFORMATION:

- Go through trash cans, dumpsters or public dumps looking for bills and other documents containing personal information.
- Take employment positions (or pay others) to steal personal information.
- Complete a change of address form to divert mail to another location.
- Steal your wallet, purse, backpack or mail and remove your credit cards, driver's license, passport, health insurance card and other items that show personal information (or take photos of those documents so you don't know they're missing).
- Steal or break into your vehicle to access your registration, insurance card or other sensitive information left in your vehicle.
- Misuse the name of a legitimate business to call or send emails (phishing) that trick you into revealing personal information.
- Send you a text message containing a link to a fraudulent website or phone number in an attempt collect your personal information (smishing).
- Pretend to offer a job, a loan or an apartment, and ask you to send personal information to "qualify".
- Find personal information you share on the internet.

HOW IDENTITY THIEVES GET YOUR INFORMATION, cont.:

- Use ATM, gas pump, or point-of-sale (POS) skimmers which steal credit and debit card information stored on the card's magnetic strip when inserted into the machine.
- Use RFID skimmers to wirelessly access credit card information from RFID-enabled cards carried in your wallet or purse from up to 2 feet away.
- Take photos of or copy credit cards at restaurants.
- Steal or find a lost smartphone or laptop that hasn't been password-protected.
- Use viruses, spyware or spoofing/dummy webpages to access your personal information.
- Access personal information through a data breach.

PROTECTING YOURSELF:

- Credit Report
  - Review your credit reports (and those of any minor children). You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. Order all three reports at once, or one report every four months (www.annualcreditreport.com or 1-877-322-8228).

- Opting Out
  - Opt out of prescreened offers of credit and insurance (www.optoutprescreen.com or 1-888-567-8688). Your initial request only places your name and address on the opt out list temporarily. To permanently opt out, you must complete and return the confirmation letter you will receive in the mail.
  - Opt out of telemarking phone calls (www.donotcall.gov or 1-888-383-1222).

- Securing Mail
  - Use a PO Box address or a locked mailbox at home.
  - Collect delivered mail promptly & suspend mail delivery during vacations.
  - Use direct deposit and online bill payments.
  - Arrange for paperless bills and statements, if possible.
  - When ordering new checks, don't have them mailed to your home unless you have a secure, locking mailbox.
  - Take outgoing mail to post office collection boxes or the post office.

- Shredding
  - Use a cross-cut shredder to dispose of all documents that show personal, financial and medical information; mix the shredded papers in with your regular trash.
  - Destroy the labels on prescription bottles before discarding.

- Your Wallet/Purse
  - Don't carry checks, birth certificate, passport, Social Security card or any document with your Social Security number in your wallet or purse unless needed that day.
  - Don't carry extra credit cards in your wallet or purse.
  - Photocopy the contents of your wallet (front and back) to aid you in the event your wallet is lost or stolen.
  - Carry your vehicle registration and insurance card in your wallet or purse instead of leaving in your vehicle.

- Your Home
  - Keep your personal information and documents in a secure place at home; if using a locking file cabinet, don't store the key nearby.
  - Consider a safe deposit box to store critical personal documents you don't need to access regularly.
  - Review your stored documents annually and shred any documents you are no longer legally required to keep.

PROTECTING YOURSELF, cont.:

- The Internet
  - Never click on links from unsolicited emails.
  - Avoid clicking on links from emails to get to your online accounts — instead type the web address (URL) of the site directly into your browser or use previously saved bookmarks.
  - Create passwords that mix letters, numbers and special characters and have a minimum of eight characters — don't use the same password for more than one account and don't share your passwords with anyone.
  - Don't always use the proper password to initially login to your computer to combat "keystroke" stealing.
  - If you shop or bank online, use websites that protect your financial information with encryption (an encrypted site has "https" at the beginning of the web address; "s" is for secure).
  - If you use a public wireless network, don't send information to any website that isn't fully encrypted.
  - Consider using a separate credit card (with a lower credit limit) for internet purchases.
  - Limit the amount of personal information you post on social media; verify that your information is available only to "friends" or people you know in real life.

- Your Computer
  - Password protect your computer.
  - Use anti-virus, anti-spyware software and a firewall on your computer.
  - Set your computer's operating system, web browser and security system to update automatically.
  - Upgrade to a newer Microsoft operating system (Vista, Windows 7, Windows 8) if your computer is running Windows XP — Microsoft stopped providing security patches for Windows XP in April 2014.
  - Avoid saving your username and password for automatic login to secure websites; be sure to log off when done.
  - Change the name (SSID) of your wireless router from the default to something unique.
  - Change your router's pre-set password; new password should be at least 8 characters long.
  - Turn off your router when you know you won't be using it.
  - Back up your files.
  - Don't leave your laptop unguarded, even for a minute — take it with you if you can, or use a cable to secure it to something heavy.
  - Don't keep passwords with your laptop or in its case.
  - Consider carrying your laptop in something less obvious than a laptop case.
  - Use an utility program to wipe your hard drive, or remove the hard drive and physically destroy it, before disposing of your computer.

- Your Smartphone
  - Password protect your smartphone.
  - Use dedicated shopping apps when shopping online instead of the phone's browser.
  - Log out of banking and other sensitive apps.
  - Never click a box asking the app to save your username/ID and password.
  - Switch off the feature that automatically connects your phone to nearby Wi-Fi networks.
  - Clear your browser history.
  - Close Bluetooth connections.
  - Install security software and keep it updated.
  - Don't store passwords, PINs, Social Security numbers, credit card or bank account information on your smartphone.
  - Delete all information and remove the SIM or memory card from your phone before disposing of it.

- Personal Security
  - Don't respond to email, text and phone messages that ask for personal information — legitimate companies don't ask for information this way.

- Personal Security, cont.
  - Don't give your personal information over the phone, through the mail or on the internet unless you initiated the contact or you are sure you know whom you are dealing with.
  - Don't give a business your social security number just because they ask (financial and government services being the exceptions) — ask if you can use another identifier or just the last four digits of your Social Security number.
  - Include only your name on your checks — don't include your Social Security number, address or even your phone number.
  - Review your bank and credit card statements and explanations of medical benefits from your health plan; report any mistakes or if statements don't come on time.

- Other Prevention Tips
  - Photocopy your passport; when traveling internationally, take a close-up photo of the country stamp in your passport and another photo of you holding the passport open showing the stamp, and email the photos to yourself.
  - Notify your credit card company if you are planning to travel out of state or out of the country.
  - Don't let anyone in a store or restaurant take your credit card out of your sight.
  - Ask your bank for an ATM card instead of a combination ATM/debit card.
  - Purchase a protective wallet for RFID skimmer protection.
  - Order and review a copy of your Social Security Earnings & Benefits Statement annually (www.ssa.gov/myaccount or 1-800-772-1213).
  - Don't set the "home" address button on your GPS to be your home address — use a familiar intersection or place of business near your home instead; hide and protect car registration and insurance information.
  - Remove your GPS and its windshield suction mount and store it out of sight when you park in public place.
  - Pay cash whenever possible, including restaurants.
  - Place a credit (security) freeze on your credit report to restrict access to your credit report and make it more difficult for identity thieves to open new accounts in your name — fees range from $5 to $10 (Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-800-680-7289).

WHAT TO DO IF YOUR IDENTITY IS STOLEN:

- Place a fraud alert on your credit report; an initial fraud alert is good for 90 days (Equifax: 1-800-525-6285; Experian: 1-888-397-3742; TransUnion: 1-800-680-7289).
- Order and review your credit report from all three credit reporting companies; report any mistakes or signs of fraud to the credit reporting company.
- File a complaint with the Federal Trade Commission (www.ftc.gov/complaint or 1-877-438-4338).
- File a police report in your home town and in the jurisdiction where the theft occurred; be sure to get a copy of the police report.
- Close any accounts that have been tampered with or opened fraudulently.
- Change all your passwords.

ADDITIONAL RESOURCES:

- Internal Revenue Service www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
- Federal Trade Commission www.idtheft.gov
- Department of Justice ID Theft www.justice.gov/criminal/fraud/websites/idtheft.html
- Center for Identity Management & Info Protection (CIMIP) www.utica.edu/academic/institutes/cimip/

The information contained herein is general in nature and is not intended to be all inclusive.

DMJ & Co., PLLC
703 Green Valley Road, Suite 201, Greensboro, NC 27408 • PO Box 9258, Greensboro, NC 27429-0258
T 336-275-9886 • F 336-275-1129 • W dmj.com

Member of CPAmerica International