

- ✓ **Put as little** personal information as possible on your checks.
  - ✓ **Review your bank statements** carefully. Match your checkbook entries against paid checks. Look for checks you didn't write. Notify your bank immediately if you find any. Then request a new account number and new checks.
  - ✓ **Carry only** a driver license, cash, a credit card, and insurance cards when you go out. Don't carry anything with PINs, account numbers, or passwords written on it. Memorize your PINs and SSN. Don't carry a checkbook or blank checks in your purse or wallet. If it is lost or stolen, the finder or thief can use the checks or print new ones and use them until you notify the bank or your account is emptied.
  - ✓ **Use ATMs that are inside a store or a bank.** These are less likely to contain devices for skimming, which is the illegal capture and use of a cardholder's financial information from an ATM transaction.
  - ✓ **If you use an outside ATM, it should be in a well-lit, well-trafficked area** and under video surveillance. Check the slot where you insert your card, the machine, and the area around it. Go to another machine if you see anything that doesn't look right.
  - ✓ **Always shield** the PIN entry pad with your hand so it can't be seen by anyone near you or by a hidden camera.
  - ✓ **Don't leave** your transaction receipts at the ATM. Take them home and use them in balancing your account. Monitor your bank statements frequently and report any unauthorized activity immediately.
  - ✓ **Report** all lost or stolen cards immediately and request cards with new numbers.
- Contact the card issuer if replacement cards aren't received in a reasonable time.
- ✓ **Never** loan your card to anyone.
  - ✓ Sign and activate new cards promptly.
  - ✓ **Bring home** all card transaction receipts. Never leave them at bank machines or counters, gasoline pumps, etc. or throw them in public trashcans. Tear them up and dispose of them at home after matching them against your monthly statements.
  - ✓ **Make sure** your bank and card companies have your latest phone numbers and e-mail address so they can contact you quickly if they suspect fraud in your accounts. And notify them in advance of any changes.
  - ✓ **Pay attention** to billing cycles and card expiration dates. Contact the card company if you miss a bill or don't get a replacement card before an expiration date.
  - ✓ **Open** your monthly statements promptly. Look for charges you didn't make. Notify your card companies or financial institutions immediately if you find any discrepancies.
  - ✓ **If you bank online**, check your balance and transactions periodically during the month.
  - ✓ Only put the last four digits of your account number on checks you write to your credit card company.
  - ✓ **Cut up old cards**, cutting through the account number and chip, before you dispose of them.
  - ✓ Ask your credit card company to stop sending blank checks.
  - ✓ **Don't let** your card out of sight. Take it to the cashier yourself.

## References

SDPD: [www.sandiego.gov/sites/default/files/identitytheftprevention.pdf](http://www.sandiego.gov/sites/default/files/identitytheftprevention.pdf)

Identity Theft Resource Center (ITRC) at [www.idtheftcenter.org](http://www.idtheftcenter.org)

Internal Revenue Service (IRS) at [www.irs.gov/newsroom/taxpayer-guide-to-identity-theft](http://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft)

Federal Trade Commission (FTC) at [www.consumer.ftc.gov/topics/identity-theft](http://www.consumer.ftc.gov/topics/identity-theft)

Privacy Rights Clearinghouse at [www.privacyrights.org/topics/id-theft-social-security-numbers](http://www.privacyrights.org/topics/id-theft-social-security-numbers)

*Revised January 17, 2018*

The City of  
**SAN DIEGO**



**SAN DIEGO POLICE DEPARTMENT**

# IDENTITY THEFT PREVENTION

## **PC 530.5 Unauthorized Use of Personal Identifying Information of another Person**

(a) Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.5, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense.

## What is Identity Theft?

Identity theft involves acquiring someone's information such as: name, address, date of birth, social security number and/or mother's maiden name in order to impersonate them. This information enables the identity thief to commit fraud which include, but are not limited to: taking over the victim's financial accounts, purchasing automobiles, applying for loans, credit cards, social security benefits, renting apartments, and establishing utility services.

## How Do Identity Thieves Get Your Personal Information?

- ✓ **By making phone calls** or sending e-mails designed to obtain personal information or offering prizes or awards.
- ✓ **Luring** you to shop or bank on unsecured websites.
- ✓ **Searching social networking** websites for personal information you may have posted.
- ✓ **Rummaging** through your trash looking for bills and other papers with information on them.
- ✓ **Skimming** credit, debit, or ATM card numbers with a device when processing your card.
- ✓ **Diverting** your billing statements to another location by completing a change-of-address form.
- ✓ **Stealing wallets** and purses
- ✓ **Stealing Mail** (Incoming and outgoing)

## How to Prevent Identity Theft?

- ✓ **Only disclose** financial or personal information when you have initiated the contact or know and trust the person you are dealing with.
- ✓ **Be careful** when talking to someone on the phone who claims to be from a financial institution where you have an account. Hang up and call the institution to find out why it is trying to reach you.
- ✓ **Put unique**, strong passwords on all your online accounts and computing devices.
- ✓ **Select password reset questions** with answers that can't be found online or from other research tools. Memorize your passwords. Don't carry them in your purse or wallet.
- ✓ **Keep your computer up to date** with the latest firewalls and anti-virus/malware software. Set the software to update automatically.
- ✓ **Protect** your smartphones, tablets, smartwatches, and other mobile devices just like you protect your computer or laptop. Disconnect your device from the Internet when you aren't using it. Use apps to help you locate your device and remotely erase the information on it if it's lost or stolen.
- ✓ **Make sure you're on a secure website page**, i.e., one that uses encryption to protect your information, when shopping or banking online. You can tell it's secure when the address on the top of your screen where the URL is displayed begins with **https** rather than **http**.
- ✓ **Keep all your personal and financial information in a secure place**, especially if you have roommates, employ outside help, or are having work done. Include copies of both sides of all the cards you carry, other account numbers, Social Security and Medicare cards, passwords, phone numbers to call to report a lost or stolen card, identity theft or other problem, etc. Cancel accounts you don't use or need.
- ✓ **Make sure** that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier's disk.
- ✓ **Shred** or tear up any documents with personal or financial information before throwing them in the trash. Use a cross-cut shredder.
- ✓ **Omit** any information that is not explicitly requested or required on forms, applications, surveys, etc.
- ✓ **Provide your SSN only when it is required** by a government agency, employer, insurance company, healthcare provider, or financial institution. Never use it for identification, especially when reporting a crime in which you are the victim. The crime report will be available to the defense if a suspect is prosecuted.
- ✓ **Do not post** personal or sensitive information, or photos on social networking websites. Use appropriate security settings for anything you do post.
- ✓ **Be suspicious** of e-mails that ask for personal or financial information, especially if they appear to come from a government agency, financial institution, software provider, or similar places. And don't click on any links in them.
- ✓ **Look** for the site's privacy policy before submitting your name, e-mail address, or other personal information on a website. This policy should state how the information will be used and whether or not the information will be distributed to other organizations.
- ✓ **Do business only** with credible companies. Check them out before supplying any information online.

- ✓ **Deposit outgoing mail** in a blue U.S. Postal Service collection box or at a Post Office, or give it directly to your mail delivery person.
- ✓ **Pick up your mail** as soon as possible after it arrives in your personal curbside box or cluster box unit. Have someone else pick it up or have your Post Office hold it until you return from a trip.
- ✓ **Have retirement benefits**, tax refunds, annuity payouts, and periodic income wired directly to your bank.
- ✓ **Contact** the issuer immediately if you don't receive a check you're expecting.
- ✓ **Have new checks mailed to your bank for collection to avoid possible theft from your mailbox.**