CALIFORNIA STATE UNIVERSITY, SAN BERNARDINO

Coyote Safety

FOR INFORMATION ABOUT OTHER CAMPUS SAFETY PROGRAMS, CALL CSU PD AT (909) 537-5165 OR EXT. 77777

IDENTITY THEFT

The crime of identity theft is on the rise. By using a variety of methods, criminals steal credit card numbers, driver's license numbers, Social Security numbers, ATM cards, telephone calling cards and other key pieces of individuals' identities. They use this information to impersonate their victims, spending as much money as they can in as short a time as possible before moving on to someone else's name and account information.

Take these preventive steps to minimize your losses in case of identity theft:

Reduce access to your personal data. To minimize the amount of information a thief can steal, do not carry extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse, except when needed.

Reduce the amount of personal information that is "out there." Consider the following: remove your name from the marketing lists of the three credit reporting bureaus—Equifax, Experian (formerly TRW) and Trans Union. This will limit the number of pre-approved credit offers that you receive. Sign up for the Direct Marketing Association's (www.the-dma.org) Mail Preference Service and the Telephone Preference Service. Have your name and address removed from the phone book and reverse directories.

When you order new checks, do not have them sent to your home's mailbox. Pick them up at the bank instead. When you pay bills, do not leave the envelopes containing your checks at your mailbox for the postal carrier to pick up. It is best to mail bills and other sensitive items at the post office rather than neighborhood drop boxes.

Passwords and PINS: When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, your birth date, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves. Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use your mother's maiden name, as that is all too easily obtained by identity thieves. Memorize all your passwords. Don't record them on anything in your wallet or purse.

Social Security numbers: Protect your Social Security number (SSN). Release it only when absolutely necessary (like tax forms, employment records, most banking, stock and property transactions).The SSN is the key to your credit and banking accounts and is the prime target of criminals. If a business requests your SSN, ask if it has an alternative number that can be used instead. If the SSN is requested by a government agency, look for the Privacy Act notice. This will tell you if your SSN is required, what will be done with it, and what happens if you refuse to provide it. Do not have your SSN printed on your checks. Order your Social Security Statement once a year to check for fraud.

TURN PAGE OVER

Responsible information handling. Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized use. Do not toss pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. Do the same with other sensitive information like credit card receipts, phone bills and so on. Discourage your bank from using the last four digits of the SSN as the PIN number they assign to customers. When you fill out loan or credit applications, find out how the company disposes of them. Store your canceled checks in a safe place. Never permit your credit card number to be written onto your checks. It's a violation of California law (California Civil Code 1725) and puts you at risk for fraud.

If You Become A Victim

If you lose your wallet, or believe that your identity has been otherwise compromised, follow these steps.

Report the crime to the police immediately. Give them as much documented evidence as possible. Get a copy of your police report. Credit card companies, your bank, and the insurance company may require you to show the report in order to verify the crime. Immediately call all your credit card issuers. Get replacement cards with new account numbers.

Call the fraud units of the three credit reporting companies—Experian (formerly TRW), Equifax and Trans Union. Report the theft of your credit cards or numbers (see below for contact information). Ask that your accounts be flagged. Also, add a victim's statement to your report. Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. Notify your bank(s) of the theft. Cancel your checking and savings accounts and obtain new account numbers. Ask the bank to issue you a secret password that must be used in every transaction. Put stop payments on any outstanding checks that you are unsure of.

If you use an ATM card for banking services, get a new card, account number and password. Do not use your old password. When creating a password, avoid such commonly used numbers as the last four digits of your Social Security number and your birth date. If you have had checks stolen or bank accounts set up fraudulently, report it to TeleCheck, National Processing Company (NPC) or Equifax.

Call your telephone, electrical, gas and water utilities. Alert them to the possibility that someone may attempt to open new service using your identification. Also contact your long distance company. You may need to cancel your long distance calling card.

You may want to change your driver's license number if someone has been using yours as identification on bad checks. When requesting a new number from the Department of Motor Vehicles, you might be asked to prove that you have been financially damaged by the theft of your driver's license. The nearest office of the Consumer Credit Counseling Service might be able to give you advice on removing fraudulent claims from your credit report. Call (800) 388-2227.

Monitor your credit reports regularly, even after your file appears to be clean. Sometimes thieves go dormant for a while, then reappear.

In dealing with the authorities and financial institutions, keep a log of all conversations, including dates and names. Send correspondence by certified mail.
Keep copies of all letters and documents. Provide your police report number to expedite reporting the crime.

Consider seeking legal counsel, especially if you have difficulty clearing up your credit history or your case is complex and involves a lot of money.

Resources

Credit reporting bureaus

Equifax	(800) 525-6285
Experian	(888) 397-3742
Trans Union	(800) 680-7289

Remember that you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit in the past 60 days, if you receive welfare benefits, or if you are unemployed.

Social Security Administration

If your SSN has been used fraudulently for employment purposes, report the problem to the Social Security Administration at (800) 269-0271.You may order your Earnings and Benefits Statement by calling (800) 772-1213. Unfortunately, the SSA has no procedures in place to deal with non-employment types of SSN fraud, such as credit application fraud. For extreme cases of identity theft, they may be willing to change your SSN.