lancaster ca
it's positively clear.

Identity Theft

Part of the Public Safety Office's "Be Secure" series

Identity theft is on the rise in America and across the world. Increased technological sophistication, combined with a growing consumer shift toward electronic transactions, has made it easier than ever for crooks to obtain and use a victim's personal or financial information for their own gain.

It is important to know what identity theft is, how to recognize it, and what steps you can take to prevent it, so that you don't become another victim.

Types of Identity Theft

There are several types of identity theft, each of which is damaging in its own right. The most common is called "theft by access card," in which a thief obtains your credit or ATM card number and creates a fake card to make ATM withdrawals or large purchases at various stores. A similar type of theft involves a thief obtaining your checking account and bank routing numbers, then printing up fake checks and cashing them or using them for purchases at various places; however this type of theft is classified as forgery, and will only be lightly touched on in this handout.

The next type of identity theft involves the use of your social security number. Often times a thief will use your SSN, combined with your name and date of birth, even sometimes your home address or telephone number, to apply for credit with multiple stores and banks, and ring up hundreds or even thousands of dollars in purchases, for which you get stuck with the bill.

Occasionally, thieves will obtain social security numbers and sell them, for purposes of employment, to illegal immigrants or those trying to evade tax collections or child support payments.

The last type of identity theft, and quite possibly the most insidious, is the complete assumption of a victim's identity, in which an ID thief lives, works, and plays as the victim. Fortunately, this typical "movie plot" is rare in real life.

Theft by Access Card

Imagine this scenario. You use your debit card everywhere to conduct your routine purchases: at the gas station, the grocery store, the dry cleaners, even the mall. You're pretty good at keeping track of how much money you have left in your account, so you only check your account once in awhile. One night you go to fill up your empty gas tank only to have your card declined. When you check your account balance, you see multiple transactions that have all overdrawn your account by over $200, resulting in several $25 overdraft fees.

There are multiple ways for thieves to obtain your card information, but the most frequent is through the use of a memory storage device attached to a card reader. Whether installed inside the card reader (more common with point-of-sale terminals inside stores, where you swipe your card) or as an attached device over the reader (more common at gas station pumps and other locations where you insert your card), the memory device captures your card information and stores it until the thief can retrieve it, or transmits it to the thief's computer. Also, smaller, less reputable internet retailers will sometimes either sell your card information or possibly have their systems hacked for it.

Here are some tips to avoid this type of ID theft:

- Only use your card at major stores that you trust. If you have the option of paying outside or going inside (such as at a gas station), go inside.
- Select the "credit" option whenever possible if using your debit card. It might not prevent the theft of the card number, but at least thieves won't have your PIN, too.
- Always check the terminal before using your card. Look for loose card readers or key pads, or for anything that looks unusual (such as a card reader that sticks out further than you remember). If you see anything suspicious, use a different terminal or payment method.
- Use a credit card instead of a debit card. Even if your information is stolen, you may not lose any money, even temporarily, with a credit card.

Banks will investigate disputed charges on checking accounts before refunding money, whereas disputed charges on credit cards do not have to paid until the card issuer investigates and determines the legitimacy of the dispute.

- Be wary when using your card to make purchases online. Always type in the URL yourself instead of clicking on a link, and check for a VeriSign, Trusteer, or other security seal (verify the certification with that company as well). If possible, use a trusted third-party payment service such as PayPal or Google Checkout that will keep your information from getting to the retailer's servers, where it could be sold or hijacked.
- Never give out sensitive information over the phone, such as your card number or your bank account and routing numbers (check-by-phone), unless you placed the call to a phone number that you got from a trusted source (not an advertisement). Don't give out this information on postcard-type return mail either, even to legitimate companies, without putting it in an envelope to mail it.

Theft of Your Social Security Number

Your social security number can be used to access all sorts of information about you and your accounts, since it is the most common way for companies to verify your identity over the phone and the internet. Credit cards and employment can be obtained with just those nine little digits, so you need to guard it as carefully as you would your paycheck.

- Never give out your social security number over the phone to anyone, including the IRS, unless you placed the call yourself using a phone number that you got from a trusted source (not an ad).
- When applying for a job, remember that even though the application asks for it, you are not required to give your social security number until you are actually hired. Job applications may be handled by multiple people not directly involved in the hiring process.
- Be wary when entering your social security number online. Only do it on websites that are certified by VeriSign, Trusteer, or another trusted internet security company, and only when you've typed in the URL yourself instead of clicking on a link.
- Keep tabs on your credit report. You are entitled to one free report per year from each credit bureau (http://www.annualcreditreport.com or (877) 322-8228) under federal law; you can order all three at once to compare details or spread them out over the year to keep up-to-date on any changes. Look for any accounts from unknown companies, addresses at which you've never lived, companies for whom you've never worked, and variations on spellings of your name.

If You've Become a Victim of Identity Theft

How will you know if you've become a victim? Look for unusual activity, that's how. Keep a regular tab on your checking and savings accounts, checking them daily if possible. Check your credit reports from all three bureaus. Keep an eye on the mail for a sudden increase in junk mail offering credit, or for mail that's all of a sudden *not* being delivered. Watch for phone calls and letters from collections agencies for accounts you didn't open. Pay attention when you apply for credit and are unexpectedly denied due to your credit score or history.

Sometimes it may take a few years for the identity theft to catch up with you, especially in the case of employment. Often the only way a victim finds out about it is when the IRS sends a letter, claiming that two or three years ago the victim underpaid their taxes or failed to report income on their tax return.

If you ever suspect or learn that you have become a victim of identity theft, there are some things you can do. Start by contacting your bank or the credit issuers (whichever is applicable) and getting copies of applications and/or transaction records. Get a copy of your credit report from each bureau and check to see if there are other discrepancies as well. If you are contacted by the IRS, ask for a Wage and Earnings Transcript to see where the fraudulent employment was obtained. All this information will be critical in helping law enforcement locate and hold accountable the criminals.

Once you have any information, call the Sheriff's Station and file a police report. Also contact the Federal Trade Commission (FTC) at (877) ID-THEFT (438-4338), or online at http://ftc.gov/bcp/edu/microsites/idtheft/.