

Lancaster Stake Personal and Family Preparedness Class

“Identity Theft”



Presented by Detective Key Budge
September 24, 2009

What is Identity Theft?

If someone is using your identifying information (name, date of birth, social security number, etc) to obtain goods, services, credit, and/or open fraudulent bank accounts, then you are a victim of Identity theft.

Identity them Laws

- All 50 States have identity theft specific laws. Most were legislated in the late 1990's. Colorado & Vermont were the last to add a specific I.D Theft law.
- Identity Theft and Assumption Deterrence Act of 1988 (Federal) identifies the true victim and seeks restitution.

Identity Theft Statutes

California Statute, 530.5 PC: The unauthorized use of personal information or any other information associated to a person. Identifying information means information that alone or in conjunction with other information identifies an individual, including:

- Name, Social Security #, DOB, and Govt. issued I.D. #.
- Unique Biometric Data, i.e.; Fingerprints, Retina, or Iris Image.
- Electronic I.D #, Address, and Routing Code.
- Telecommunication identifying information or access device (account & pin #s, etc.). Or in conjunction with another telecommunication access device may be used to:
- Obtain money, goods, services, or things of value, without the person's consent.

Punishable as a Felony

Identity Theft Statistics

- The Federal Trade Commissions # 1 fraud complaint received.
- 5.5% of American's are already victims.
- 8.3 Million American's victimized in 2006. Costing consumers \$20 Billion Dollars.
- Costing Businesses \$96.9 Billion.
- Roughly 3,000 new victims each day nationwide.

Who Are the Victims?

The most victimized demographic is men & women between the ages of 30-39. Although identity theft perpetrators are not gender or age specific.

- Busy personal schedules.
- Work Hard / Play Hard.
- Enjoy buying toys (boats, cars, etc.)
- Do not spend enough time checking their finances.

Ultimately the Financial Institutions & Retail Businesses bear the weight of the losses.

How Identity Theft Occurs

- Lost or Stolen Wallet/Purse.
- Mail Theft.
- “Dumpster Divers” in Business & Residential trash receptacles.
- Stolen Vehicles.
- Residential & Business Burglaries.
- E-mail Scams.

What’s in your Wallet?

- Drivers License (Some States use Social Security Number as DL #)
- Social Security Card
- Credit Cards (Some W/PIN #'s)
- Medical Insurance Card

The new breed of ATM Thieves



Skimmer being installed on front of existing bank card slot.

The PIN reading Camera being installed on the ATM is housed in an innocent looking leaflet enclosure.



The equipment as it appears installed over the normal ATM bank slot.

The camera shown installed and ready to capture PINs by looking down on the keypad as you enter number



What Gets Stolen?

Vehicles

- Wallets / Purses
- Briefcases & Back packs
- Vehicle Registration
- Garage Door Remote Controls
- Laptops

Briefcase, Back pack, Purse, Wallet

- Drivers License or ID Card
- Social Security Cards (yes many people still carry their SS cards).
- Debit & Credit cards (with pin numbers).
- Health Care Insurance Cards (social security number usually on card).

Residential Burglaries

- Wallets & Purses.
- Mail & Billing Statements.
- Home Computers Hard Drives.
- Laptop Computers, PDA's.
- Personal Documents(birth, marriage, death certificates– any doc w/name and d.o.b., etc)
- Home Electronics, Safes, Guns, Jewelry, & Cash (remember they are crooks)
- Vehicles & Extra Keys

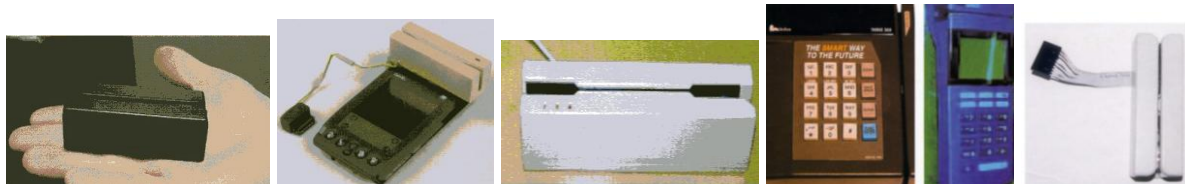
Businesses

- Credit Applications, Computers, Files & Records, Client Lists, & Accounting Records.

Employees

- Remove Credit info from files, and sell or trade for drugs.

SKIMMING & CARD STRIPE



What Happens with Stolen Identity?

- Used immediately by thief.
- Trade personal information for drugs.
- Obtain credit or products.
- Counterfeit or alter I.D. cards.
- Assume victims identity, and purchase goods.
- Network the identity information.

Where It all Begins



Suspect Trends

- Utilizing hotel rooms to purchase on line products.
- Deliver overnight to abandoned home or hotel.
- They meet the delivery truck in the parking lot.
- Sold or traded within minutes of receiving the merchandise.

Victim Responsibilities

Once you discover you are a victim of identity theft you should notify the following:

- Contact the Credit bureaus
- Contact Your Creditors
- Contact Law Enforcement
- Complete victim affidavit.
- Alert Credit Reporting Agencies.
- Keep a diary of who, what, when, where, why & how.
- Keep in contact with investigator, “Squeaky Wheel” theory.
- Request copy of credit report quarterly.

Plan on 200+ hours of your own time to clean up credit nightmare.

Costs up to \$1,000 – \$1,500 in expenses or loss.

When Dealing with Financial Institutions

- Streamline investigation time line.
- Provide information as needed.
- Contact customer/victim, and confirm fraudulent activity. A fraud occurred, the suspects have no expectation of privacy.
- Provide Law Enforcement with direct line phone numbers.
- Timely communication is a key ingredient for an effective investigation.

Reporting ID Theft

*In dealing with the authorities and financial institutions, **keep a log** of all conversations, including dates, times, names, and phone numbers. Note the time spent and any expenses incurred. Confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.*

Once you discover you are a victim of identity theft you should notify the following:

The First Step is Contacting the Credit Bureaus.

- Immediately call the fraud units of the three credit reporting companies– Experian, Equifax, and Trans Union. Report the theft of your credit cards or numbers. The phone numbers are provided at the end of this brochure. Ask that your account be flagged. Also, add a victim’s statement to your report, up to 100 words. (“My ID has been used to apply for credit fraudulently. Contact me at (*your telephone number*) to verify all applications.”) Be
- Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary. *Be aware that these measures may not entirely stop new fraudulent accounts from being opened by the imposter. Ask the credit bureaus in writing to provide you with a free copy every few months so you can monitor your credit report.* Ask the credit bureaus for names and phone numbers of credit grantors with whom fraudulent accounts have been opened. Ask the credit bureaus to remove the inquiries that have been generated due to the fraudulent access. You may also ask the credit bureaus to notify those who have received your credit report in the last six months in order to alert them to the disputed and erroneous information (two years for employers).

Equifax:

- Roosevelt Blvd, St. Petersburg FL 33716-2202
- Report Fraud: Call (800) 290-8749 and write to address above.
- Order a credit report: (800) 685-1111.
- Opt out of pre-approve offers of credit; (888) 5OPTOUT or (888) 567-8688.

Experian (formerly TRW):

- PO box 1017, Allen, TX 75013
- Report Fraud: Call (800) 301-7195 or (888) 397-3742 and write to address above.
- Order a credit report: (888) 397-3742.
- Opt out of pre-approved offers of credit and marketing lists: (888) 567-8688

Trans Union: PO Box 390, Springfield, PA 19064

- Report Fraud: (800) 680-7289
- Consumer Relations: (800) 916-8800 and write to
- Fraud Victim Assistance Division, PO Box 6790, Fullerton, CA 92834-6790
- Order Credit Report: (888) 680-7293
- Remember, if you have been the victim of credit fraud or are denied credit you are entitled to a free credit report. If you are a victim of fraud, be sure to ask the credit bureaus for free copies. They will often provide them.

The Second Step is Contacting Your Creditors

- Contact all creditors immediately with whom your name has been used fraudulently- by phone **and** in writing. Get replacement cards with new account numbers for your own accounts that have been used fraudulently. Ask that old accounts be processed as “account closed at consumer’s request.” (This is better than “card lost or stolen” when this statement is reported to credit bureaus, it can be interpreted as blaming you for the loss.) Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.
- **Creditors requirement to report fraud.** You may be asked by banks and credit grantors to fill out and notarize fraud affidavits, which could become costly. The law does not require that a notarized affidavit be provided to creditors. A written statement and supporting documentation should be enough (unless the creditor offers to pay for the notary).

The Third Step is Contacting Law Enforcement

Report the crime to the law enforcement agency with jurisdiction in your case. Give them as much documented evidence as possible. Get a copy of your police report. Keep the report number of your police report handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report to verify the crime. Some police departments have been known to resist writing reports on such crimes. Prior to January 1st, 1998, the creditors (credit card companies, banks, etc.) were the only “legal” victims of Credit Fraud/Identity Theft. California Penal Code Section 530.5 went into effect on January 1st, 1998, thus giving legal standing to individual victims. Some police departments have not yet received training in the new laws of Identity Theft. Be persistent!

How Does Law Enforcement Investigate?

- Victim notifies law enforcement after discovering the theft of wallet, vehicle, or home.
- Victim notifies law enforcement when applying for credit, sometimes years after the fraud occurred.
- Victim notifies financial institution, and is told to obtain a police report.
- Retail store notifies law enforcement of suspect obtaining goods fraudulently.
- We get lucky.

The Investigation

Uniform Officer / Deputy Responds

- Takes initial report.
- Gathers evidence.
- Attempts to locate / interview witnesses.
- Look for suspects.

Cases Reviewed for Assignments

- Supervisors determine if there is workable information, and assign the case to a detective.
- No workable information, means case placed in pending .

Detective Receives Case

- If suspect in custody, case assigned within 1–24 hours of arrest.
- Detective has 48 hours from arrest to complete investigation and present to DA.

Detective's Investigation

- Review original report.
- Contact victim, confirm information.
- Give victim homework
- Contact Financial Institutions.

Track down fraud investigator that can confirm information and provide follow up support.

- Review evidence.
- Interview suspects.
- Prepare search warrants if needed, and write supplemental reports.
- Track down unknowing victims.
- Present investigation to District Attorney.
-

How does Law Enforcement address the increasing I. D. Theft Crime Rate?

- Hire more police officers / investigators.
- Develop Task Force Units where multiple agencies work together
Local Police, Sheriff, State, and Federal Investigators sharing resources.
- Local Special Investigations Detail Units. "S.I.D." is an effective local level answer.
Consists of a team of 2–6 investigators, working together on special projects.
- Corporate Technology Grants.
- Equipment donations

What Can we Do?

- Train the public sector on how to identify fraud suspects & documents.
- Train the public on how to protect their information & identities.
- Work with the media on informing the public on new crime trends.
- Alert businesses to properly dispose of client information.

Roadblocks for Investigators

- Budget shortfalls.
- Lack of experienced investigators.
- Communication flow with Financial Institutions.
- Work overload (too many cases).
- Uncooperative victims.
- Technology

OTHER CONCERNS IN ID THEFT

Stolen Checks

If you have had checks stolen or bank accounts set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks that you are unsure of. Cancel your checking and savings accounts and obtain new account numbers. Give the bank a secret password for your account (not your mother's maiden name).

To report fraudulent use of your checks:

- ✓ CheckRite: (800) 766-2748
- ✓ CrossCheck: (800)843-0760
- ✓ Chexsystems: (800) 428-9623
- ✓ Equifax: (800) 437-5120
- ✓ International Check Svcs: (800) 526-5380
- ✓ SCAN: (800) 262-7771
- ✓ Telecheck: (800) 710-9898

ATM Cards

If your ATM card has been stolen or is compromised, get a new card, account number, and password. Do not use your old password. When creating a password, don't use common numbers like the last four digits of your social security number or your birth date.

Fraudulent change of address

Notify the local Postal Inspector if you suspect an identity thief has filed a change of address with the post office or has used the mail to commit credit or bank fraud. Find out where the fraudulent credit cards were sent. Notify the local Postmaster for the address to forward all mail in your name to your own address. You may also need to talk to the mail carrier.

Social Security number misuse

Call the Social Security Administration to report fraudulent use of your social security number. As a last resort, you might want to change the number. The SSA will only change it if you fit their fraud victim criteria. Also order a copy of your Earnings and Benefits Statement and check it for accuracy. To Report Fraud: (800) 269-0271

To Order your Earnings and Benefits Statement: (800) 772-1213

Passports

If you have a passport, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.

Phone Service

If your long distance calling card has been stolen or you discover fraudulent charges on your bill, cancel the account and open a new one. Provide a password which must be used anytime the account is changed.

Driver License number misuse

You may need to change your driver's license number if someone is using yours as identification on bad checks. Call the state office of the Department of Motor Vehicles (DMV) to see if another license was issued in your name. Put a fraud alert on your license. Go to your local DMV to request a new number. Also, fill out the DMV's complaint form to begin the fraud investigation process. Send supporting documents with the complaint form to the nearest DMV investigation office.

False Civil and Criminal Judgments

If a civil judgment has been entered in your name for actions taken by your imposter, contact the court where the judgment was entered and report that you are a victim of identity theft. If you are wrongfully prosecuted for criminal charges, contact the state Department of Justice and the FBI. Ask how to clear your name.

Let's Review

Identity Theft Prevention

- ☑ Shred all documents. The cross shred method is preferred.
- ☑ Do not carry extra credit cards.
- ☑ Don't give personal information over the telephone, or internet.
- ☑ Remove mail promptly from mailbox.
- ☑ Deposit outgoing mail at Post Office.
- ☑ Don't leave receipts at the point of sale.
- ☑ Memorize pins, social security numbers, and passwords.
- ☑ Sign all new credit cards.
- ☑ Match receipts to monthly billing statements.
- ☑ Notify Financial Institutions in advance of address changes.

Identity Protection Services

Private companies offer a variety of choices from \$9.95 a month on up. It helps with peace of mind. It also provides a head start on some investigations. PC Software designed to help the victim understand the totality of the damage and how to repair the damage.

Life Lock: LifeLock.com 1-800-390-2119

Once you discover you are a victim of identity theft you should notify the following:

- Contact the Credit bureaus
- Contact Your Creditors
- Contact Law Enforcement
- Complete victim affidavit.
- Alert Credit Reporting Agencies.
- Keep a diary of who, what, when, where, why & how.
- Keep in contact with investigator, "Squeaky Wheel" theory.
- Request copy of credit report quarterly.

Plan on 200+ hours of your own time to clean up credit nightmare.

Costs up to \$1,000 – \$1,500 in expenses or loss.

Resources

Other Useful Resources:

- Federal Government Information Center:
Call (800) 688-9889 for help in obtaining government agency phone numbers.
- Federal Trade Commission (877) FTC-HELP for help in any type of consumer complaint
- FTC Consumer's Page www.consumer.gov/idtheft
- Federal Trade Commission www.consumer.gov/idtheft (877) 438-4338
- Privacy Rights Clearinghouse www.privacyrights.org

To remove your name from mail and phone lists:

- Direct Marketing Association Mail Preference Service
PO Box 9008, Farmingdale, NY 11735
- Telephone Preference Service, PO Box 9014, Farmingdale, NY 11735

Federal Laws

- Identity Theft and Assumption Deterrence Act: www.ftc.gov/os/statutes
- Fair Credit Reporting Act (FCRA) www.ftc.gov/os/statutes

State of California

- Unauthorized Use of Personal Identifying Information: 530.5 PC

Useful Internet Locations

- Federal Trade Commission www.ftc.gov
- California Department of Consumer Affairs www.dca.ca.gov
- Los Angeles County Department of Consumer Affairs: consumer-affairs.co.la.ca.us
- Type "Identity Theft" into your web browser
- Forward Internet scam emails to the FTC uce@ftc.gov

I.D. Theft...Are You Next?

KEY L. BUDGE

L.A.S.D Detective

(661) 949-6525

klbudge@lasd.org keyconsultants.org

Alerts Consumers about U.S. Census Workers: Be Cooperative, But Cautious!

For years, Better Business Bureau has educated consumers about not giving out personal information over the telephone or to anyone who shows up at their front door. With the U.S. Census process beginning, BBB advises people to be cooperative, but cautious, so as not to become a victim of fraud or identity theft.

The first phase of the 2010 U.S. Census is under way as workers have begun verifying the addresses of households across the country. Eventually, more than 140,000 U.S. Census workers will count every person in the United States and will gather information about every person living at each address including name, age, gender, race and other relevant data.

"Most people are rightfully cautious and won't give out personal information to unsolicited phone callers or visitors, however the Census is an exception to the rule," said Steve Cox, BBB spokesperson. "Unfortunately, scammers know that the public is more willing to share personal data when taking part in the Census and they have an opportunity to ply their trade by posing as a government employee and soliciting sensitive financial information."

The Census data will be used to allocate more than \$300 billion in federal funds every year, as well as determine a State's number of Congressional representatives. Households are actually required by law to respond to the Census Bureau's request for information.

During the U.S. Census, households will be contacted by mail, telephone or visited by a U.S. Census worker who will inquire about the number of people living in the house. Unfortunately, people may also be contacted by scammers who are impersonating Census workers in order to gain access to sensitive financial information such as Social Security, bank account or credit card numbers. Law enforcement in several states have issued warnings that scammers are already posing as Census Bureau employees and knocking on doors asking for donations and Social Security numbers.

The big question is - how do you tell the difference between a U.S. Census worker and a con artist? BBB offers the following advice:

- If a U.S. Census worker knocks on your door, they will have a badge, a handheld device, a Census Bureau canvas bag and a confidentiality notice. Ask to see their identification and their badge before answering their questions. However, you should never invite anyone you don't know into your home.
- Census workers are currently only knocking on doors to verify address information. Do not give your Social Security number, credit card or banking information to anyone, even if they claim they need it for the U.S. Census. While the Census Bureau might ask for basic financial information, such as a salary range, it will not ask for Social Security, bank account or credit card numbers nor will employees solicit donations.
- Eventually, Census workers may contact you by telephone, mail or in person at home. However, they will not contact you by e-mail, so be on the look out for e-mail scams impersonating the Census. Never click on a link or open any attachments in an e-mail that are supposedly from the U.S. Census Bureau.

For more advice on avoiding identity theft and fraud, visit www.bbb.org