Identity Theft and Financial Crimes

The West Sacramento Police Department investigates identity theft and many different types of financial crimes. Identity theft covers a broad variety of financial crimes that are related to the fraudulent use of your personal identifying information. Your personal information includes your name, date of birth, address, telephone number, health insurance identification number, taxpayer identification number, school identification number, state or federal driver's license or identification number, social security number, place of employment, employee identification number, mother's maiden name, checking and savings account number, credit card numbers, PIN (personal identification number) or password, alien registration number, government passport number, or information contained in a birth or death certificate.

Criminals can obtain your personal identifying information in a variety of ways. Some common methods include:

- **Theft –** This can include mail theft, vehicle burglaries, residential burglaries, commercial burglaries, or purse snatch/pick pocket crimes.

- **Trash** - Searching through residential and business trash for any personal information, financial statements, or carelessly discarded mail.

- **Cold calling** – When a criminal calls you pretending to be with a company and asks you for your personal information over the phone, usually with the promise of a phony "rebate" or "refund" they claim you are owed or to "update" your account.

- **Employees** – Any place of business or service industry where you use your bank account, credit card, or other personal identifying information has the potential to be a point of compromise for your information. Employees who are "ID Thieves" may steal your information from their place of employment for their own use or sell it to a third party for money or narcotics.

- **Card Skimming** – Criminals who set up card reading devices at gas stations, ATM machines, or in a business to capture your bank or credit card information for future use.

- **Internet** – E-Mails that appear to be from legitimate business asking you to "update your account", when they are in fact phony e-mails just meant to steal your information. Also, "War Driving" a term for criminals who attempt to access your information by picking up your wireless internet signals from your home or any area where wireless access is allowed.

- **Family Members/Co-Workers** – These persons may have easy access to your information, and those suffering from addictions to drugs, alcohol, gambling, or shopping may be tempted to victimize their own friends and family.

What happens with your information?

Once a criminal has your information they can use it for themselves, sell your information to others, or trade it for narcotics or property. Depending upon the level of sophistication of the crime they may do an account takeover, where they start using your account without your permission. They may even change the mailing address for your account order replacement credit cards and/or checks, or make checks/credit cards using your account information. Criminals may also apply for new accounts, make phony identifications, driver's licenses, or social security cards, or set up rentals, leases, or utility accounts with your information.

How can you protect yourself?

- If possible get a locking mailbox, collect your mail everyday, and deposit outgoing mail into a U.S. Mail mailbox or at the post office.

- Do not leave any financial or personal identifying information in your vehicles.

- Attempt to secure your financial and personal identifying information documents in a locked file cabinet at your home or business.

- Use a shredder for your trash, and shred all credit card offers, billing statements, bank statements, or anything else containing your personal identifying information before throwing it away.

- Do not carry all of your credit cards and your social security card with you. Keep only the card(s) you need, and secure the rest in a safe place or safety deposit box.

- Do not preprint your checks with your license number, social security number, or phone number.
- Do not reveal personal information over the phone unless you are sure you can verify who you are dealing with. If you receive a suspected "cold call" for a "refund" or "account verification" contact the business or financial institution by calling the phone number listed on your statement or in the phone book.

- Be selective in where you do business. Try to use only one credit/debit card or cash for your purchases to limit the exposure of your information. Always be mindful that it is not safe to carry large sums of cash.

- Use only one credit card for your online purchases and use secure sites only.

- Review your monthly billing statements for fraudulent charges, and report them immediately to your financial institution.

- Check your credit report at least once per year for any fraudulent activity.

- Install security software on your computer, and encryption if you are using wireless internet.

What should you do if you become a victim of identity theft?

- Contact the fraud departments of the three major credit bureaus, advise them that you are an identity theft victim, and would like a fraud alert placed on your file. This will require creditors to call you before changing your accounts or establishing any new accounts.

Equifax	**Experian**	**TransUnion**
www.equifax.com	www.experian.com	www.transunion.com
Credit Reports	Credit Reports	Credit Reports
1-800-685-1111	1-888-397-3742	1-800-916-8800
Reporting Fraud	Reporting Fraud	Reporting Fraud
1-800-525-6285	1-888-397-3742	1-800-680-7289

- Contact the fraud departments for any of your accounts that have been compromised. Demand that the old account be closed, and that a new account number be established. Your old account number may be in the possession of many different thieves, and the fraud could continue.

- File a police report. Per California law the agency where you live shall take a police report from you for identity theft regardless of where the fraudulent transactions are occurring. You are also entitled to a free copy of the police report. The West Sacramento Police Department will provide you with the face page of the report. This will contain the case number, the date and time of your report, a summary of your case, and will have you listed as the victim/reporting party. Copies of reports are available at the West Sacramento Police Department Monday through Friday from 8:00 a.m. until 5:00 p.m. Identification is required to obtain the report to further protect your identity.

- Keep a log and records of who you speak to, papers and reports you file, and what steps you take to clear your name and credit.

- Register with the Federal Trade Commission as a victim of identity theft.

For additional tips and resources please visit the links below:

State of California	Federal Government	CA Office the Attorney General
Office of Privacy Protection	Federal Trade Commission	http://ag.ca.gov/idtheft/tips.htm
www.privacyprotection.ca.gov	www.ftc.gov	