

What is Identity Theft?

Identity theft involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number, or mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which may include taking over a victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards, social security benefits, or renting apartments and establishing services with utility and phone companies.

What to do if you become a victim

- Set up a folder to keep a detailed history of this crime.
- Keep a log of all your contacts and make copies of all documents.
- Notify the US Postal Inspector if your mail has been stolen or tampered with.
 - o US Postal Inspection Service
1 (626) 405-1200
 - o www.usps.gov/postalinspectors
- Contact the Federal Trade Commission to report the problem
 - o www.ftc.gov – The FTC is the federal clearinghouse for complaints by victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result from identity theft. Their hotline telephone number is 1 (887) IDTHEFT, or 1 (877) 438-4338.
- Alert your banks to flag your accounts and contact you to confirm any unusual activity. Request a change of PIN and a new password.

- Contact the Social Security Administration's Fraud Hotline at 1 (800) 269-0271
- Contact the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the DMV's complaint form to begin the fraud investigation process.
- If you have any checks stolen or bank accounts set up fraudulently, report it to the following companies:
 - o Nat'l Check Fraud at 1 (843) 571-2143
 - o SCAN at 1 (800) 262-7771
 - o Tele-Check at 1 (800) 710-9898
 - o CheckRite at 1 (800) 638-4600
 - o Equifax-Telecredit at 1 (800) 437-5120
 - o Chex Systems at 1 (800) 328-5121
 - o NPC at 1 (800) 526-5380
- Call each of the three credit bureaus' fraud units to report the identity theft. Ask to have a "Fraud Alert" placed on your credit file. This requires creditors to call you before opening new accounts

Equifax Credit Information Services
PO Box 740256, Atlanta, Georgia 30374
Consumer Fraud Div 1 (800) 525-6285
FAX 1 (770) 375-2821
To order your report 1 (800) 685-1111
www.equifax.com

Experian Consumer Services
PO Box 9530, Allen, Texas 75013
To report fraud 1 (888) 397-3742
To order your credit report 1 (888) 397-3742
www.experian.com

TransUnion Fraud Victim Assist Center
PO Box 6790, Fullerton CA 92834
To report fraud 1 (800) 680-7289
FAX 1 (714) 447-6034
To order your credit report 1 (800) 888-4213
www.transunion.com

- Obtain description of suspect (if known) and contact info for any witnesses
- Retain documentation of your financial loss
- Contact all creditors, by phone AND in writing, to inform them of the problem.

Sample "Courtesy Notice"

(Date)

(Creditor or Collection Agency Name)

On (date), I received your letter demanding payment of (\$ amount). I did not open this account or incur this unpaid balance. Someone other than me wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/service to someone other than me.

Your company is a victim and should file a police report in the appropriate jurisdiction.

I filed an identity theft report with the San Luis Obispo Police Department. The case number is

Please refer to the attached copy for details.

Sincerely,
(your name and address)



SAN LUIS OBISPO POLICE DEPARTMENT

Internet and On-Line Services

Do not respond to unsolicited e-mails, requests for account updates, or other requests for personal information. Banks and credit institutions will not request personal information via e-mail. Contact them by phone if you have any concerns or questions.

When making on-line purchases, do not provide your personal information unless you are using a "secure" website. Check for the padlock symbol in the web browser or an "S" in the web address at the beginning, i.e., <https://www.wellsfargo.com/>

Informational Websites

Federal Trade Commission
www.ftc.gov
www.consumer.gov/idtheft/

California Department of Consumer Affairs
www.dca.ca.gov

Privacy Rights Clearing House
www.privacyrights.org

U.S. Postal Inspection Service
www.usps.gov/postalinspectors

International Association of Financial Crimes
Investigators
www.iafci.org (go to links)

Equifax Credit Information Services
www.equifax.com

Experian Consumer Services
www.experian.com

TransUnion Fraud Victim Assistance Center
www.transunion.com

Preventative Actions

- Promptly remove mail from your mailbox after delivery
- Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave in unsecured mail receptacle.
- Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or bank PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessary.
- Shred pre-approved credit applications, credit card receipts, bills, and other financial information before discarding them in the trash or recycling bin.
- Opt out of pre-screened credit or insurance offer mailing lists from Experian, Innovis, TransUnion, and Equifax by calling:
- 1 (888) 5OPT-OUT or 1 (888) 567-8688
- Have your name and phone number removed from mail and phone lists by writing to:

Direct Marketing Association

- o *Mail Preference Service*
- o PO Box 9008, Farmingdale NY 11735

- o *Telephone Preference Service*
- o PO Box 9014, Farmingdale NY 11735

- Empty your wallet of extra credit cards and IDs, or better yet, cancel the ones you do not use and maintain a list of the ones you do.
- Order your credit report from the three credit bureaus once a year to check for fraudulent activity or other discrepancies.
- Memorize your social security number and all of your passwords. Do not record them on anything in your wallet or purse.
- Never leave receipts at bank machines, bank counters, trash receptacles, or gasoline pumps. Keep track of all your paperwork. When you no longer need it, destroy it.
- Sign all credit cards upon receipt and save all credit card receipts and match them against your monthly bills.
- Be conscious of normal receipt of routine financial statements. Contact the sender if they are not received in a timely manner.
- Notify credit card companies and financial institutions in advance of any change of address or phone number.
- Never loan your credit cards to anyone else and report all lost or stolen credit cards immediately.
- Never put your credit card or other financial account number on a postcard or on the outside of an envelope.
- If you have applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.

- Beware of all mail and telephone solicitations disguised as promotions offering instant prizes or awards. They are designed solely to obtain your personal information and/or credit card numbers.

Your SLOPD Case Number is:

Make note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report. Depending on the location ("jurisdiction") of where the crime occurred (where the goods or services were obtained or delivered), a SLOPD investigator may or may not be assigned to this case.

If the crime occurred in our jurisdiction and there are workable leads, such as witnesses or suspect information, an investigator will be assigned to the case.

San Luis Obispo Police Department
Investigative Division
1042 Walnut Street
San Luis Obispo CA 93401
(805) 781-7317, then press "2"

IDENTITY THEFT A Quick Reference Guide



San Luis Obispo Police Department

Penal Code Section 530.5 **Unauthorized Use of Personal Identifying Information**

(Rev 08/06)

530.5(a) PC – Every person who willfully obtains personal identifying information ... of another person and uses that information for any unlawful purpose, including to obtain or attempt to obtain credit, goods, services, or medical information in the name of the other person without consent of that person, is guilty of a public offense.