What If I am a Victim?

If your identity is stolen act quickly and effectively! Be sure to keep a list of all communications.

1. Contact the fraud depts. of the three major credit bureaus (see previous page for numbers).

2. Notify bankers and creditors and close accounts you feel were tampered with.

3. File a police report and get a written copy of your report.

4. Call the FTC Identity Theft Hotline at 877-ID-THEFT or go online www.consumer.gov/idtheft to file a complaint.

U.S. Secret Service, U.S. Postal Inspection Service, the FBI and local law enforcement investigate identity theft and computer fraud complaints.

U.S. Attorney's Office Victim Witness Program

450 Golden Gate Avenue
11th Floor
San Francisco, CA 94102
Phone: 800.273.9606
Fax: 415.436.7234

280 S. First Street, #371
San Jose, CA 95113
Phone: 888.396.3270
Fax: 408.436.5066

1301 Clay Street, 340S
Oakland, CA 94612
Phone: 888.396.3270
Fax: 510.637.3724

www.usdoj.gov/usao/can/home.html

United States Attorney's Office

How Identity Theft Occurs, How to Restore Your Good Name and How To Stop It From Happening Again!

Identity Crime

Common ways thieves steal your ID are through regular mail, Internet auction sites and online shopping

How ID Theft Occurs?

Identity theft occurs when a thief steals your personal information, such as a credit card account number, social security number or driver's license number. They then open up accounts in your name and run up charges. Or, they will incur charges on your existing accounts.

The most common types of identity theft occur through stealing your mail and using the Internet. 2002 statistics show the fraud trends.

- Credit Card Fraud – 42%
- Phone & Utilities Fraud – 22%
- Bank Fraud – 17%
- Employment Fraud - 9%
- Benefits/Gov't. Fraud – 8%
- Loan Fraud – 6%

How Do I Protect Myself?

- Never give your checking account, credit card, or SSN to **unknown** callers or **unknown** Internet retailers. Be aware of "phishing" Emails that appear to be from known retailers asking you for updated account & credit card information. These may be bogus Emails and websites collecting your personal data. Double check with the business directly before updating your data.
- Watch for interruptions in billing cycles (missing mail).
- Get a locked mailbox and retrieve mail the day of delivery.
- Review your financial accounts and credit reports regularly.
- Shred all papers containing personal information before throwing them away.
- Use non-sensible PINs and don't write them on your cards.

- Only do business with reputable companies.
- Use secure websites to place orders (the https:// signifies "secure").
- Update your virus protection software regularly.
- Get off mailing lists by calling 888-5-OPTOUT to stop receiving credit card offers.
- Opt out of company sharing information with outsiders.
- Be wary of calls requesting updated or clarifying information.

If you are a victim of ID Crime, contact the fraud departments of the three major credit bureaus, report the theft and ask for a "fraud alert" to be placed on your file and that no new credit be granted without your approval.

Equifax: (800) 525-6285

Experian: (888) 397-3742

Trans Union: (800) 680-7289