



# The Basics of Identity Theft

Your wallet is missing. Thousands of dollars have been charged to your credit cards, your checking account is empty, and loans you never took out appear on your credit report. What happened? You've been a victim of identity theft – an increasingly common and inventive crime.

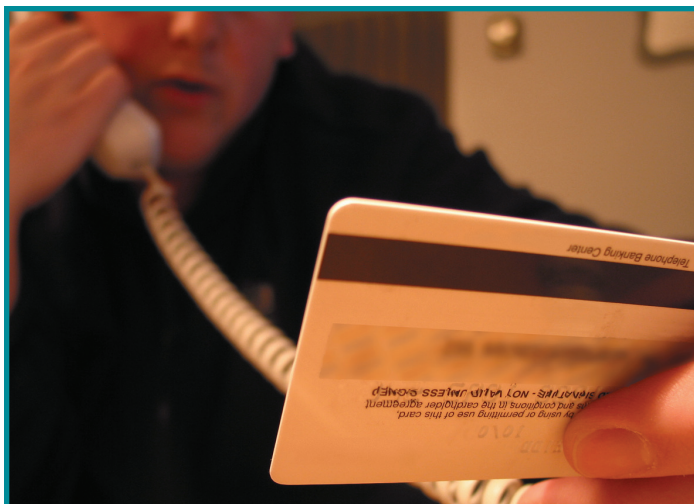
Identity theft occurs when someone uses your personal information to commit fraud or other crimes. It may also involve computer fraud, mail fraud, wire fraud, and financial institution fraud.



Fortunately, there are preventative measures you can take to substantially reduce the chance of identity theft occurring, as well as steps to recover from any damage if you are a victim.

595 Market Street, 15th Floor, San Francisco, CA 94105

800.777.7526 • [www.cccssf.org](http://www.cccssf.org)



## Common Practices

### How Your Information is Obtained

Thieves use a variety of illegal techniques to obtain identity information. They may:

- Take mail from a mailbox, or divert mail to another location by filling out a change of address form.
- Go through trash to find identification and financial documents.
- Access credit reports by posing as landlords or employers.
- Hack into personal computers.
- Pose as legitimate companies or government agencies to request personal information via email (called phishing) or text message (called smishing).
- Steal hard copy or electronic files from your workplace.
- Stand close to you at the ATM to learn your Personal Identification Number (PIN).
- Attach a skimmer to an ATM to capture the card number and PIN.

### How Your Information May Be Used

Once identity thieves have your personal information, they may use it to:

- Charge on existing credit accounts or open new credit accounts in your name.

- Use existing or open new checking accounts in your name and write bad checks.
- Establish phone or wireless service in your name.
- Use your debit cards or counterfeit checks to drain your checking account.
- Take out loans to buy cars and other big ticket items.

## Preventing Identity Theft

There are many ways to protect your private information from fraud. Some tasks take a bit of effort, be aware that cleaning up the mess identity thieves leave behind is far more difficult and time-consuming.

### Credit Reports

At least annually, check your credit report from each of the three major credit bureaus for fraudulent activity. Through the Annual Credit Report Request Service, you are entitled to one free report per year from each of the three credit bureaus. You may be entitled to additional free reports if you've been a victim of identity theft. If you find inaccuracies on your report, dispute them immediately.

### Personal Identity Information

- Keep all identification and financial documents in a safe and private place.
- Provide personal information only when you know how it will be used, you are certain it won't be shared, and you've initiated contact and know who you're dealing with.
- Make all passwords hard to guess by using a complex combination of numbers and upper and lower case letters.
- Request a vacation hold if you can't pick up your mail and deposit outgoing mail in post office collection boxes or at your local post office.
- Be aware of your workplace's security procedures and keep your purse or wallet in a safe place.
- Do not carry your Social Security card or have it or your driver license number printed on your

checks. Share this information only when necessary and to those you trust.

### **Credit Card, ATM, Debit Cards & Checking Accounts**

- Photocopy both sides of your credit cards so you have all the account numbers, expiration dates and phone numbers, and keep the copies in a safe place. Carry only those cards you really need and cancel unused accounts.
- Shred all statements and pre-approved credit card offers with a crosscut shredder.
- Be aware of people behind you at the ATM, or anywhere else you swipe your card. If you give your credit or debit card to someone for a transaction, watch them swipe it and inspect the receipt for accuracy.
- Know your billing cycles and contact your creditors if your statements don't arrive on time.
- Know where your checkbook is at all times. When you write a check, be sure to print firmly and use indelible ink. Check your account statement for fraudulent activity.
- Examine your transactions online or on your statements each month.

### **Computer**

- Update your virus protection software periodically, and after every new virus alert is announced. Also, use a firewall program to prevent your computer from being accessible to hackers.
- Do not download files or open hyperlinks sent from people you don't know.
- Use a secure browser to guard the security of your online transactions. Enter personal and financial information only when there is a "lock" icon on the browser's status bar and look for the URL to read "https" versus "http".
- If you must store personal and financial information on your laptop, use a strong password



– one that is a hard-to-guess combination of upper and lower case letters and numbers, don't use an automatic log-in feature, and always log off when you're finished.

### **Recovery Guide**

If you are a victim of identity theft, understand that minimizing damage will take patience and a systematic approach. However, the sooner and more aggressively you deal with the problem, the faster you will see results.

To start, commit yourself to becoming and remaining organized. Since you will be communicating with a lot of people and have many tasks to complete, use the Action Log to keep track. Keep copies of all letters, file paperwork promptly, and store everything in a safe and accessible place.

### **Creditors and Financial Institutions**

- If accounts have been used or opened illegally, contact your creditors immediately. For any compromised account, you should get a new account number and card. You may need to provide the creditor with a police report or the Federal Trade Commission's Identity Theft Victim's Complaint and Affidavit. Monitor all future account statements carefully for evidence of new fraud.
- If a collection agency attempts to collect on a fraudulent account, explain (in writing) that you

are a victim of identity theft and not responsible for the debt. Ask that they confirm in writing that you do not owe the balance and that the account has been closed.

- For checking account fraud, contact your financial institution to place stop payments on any outstanding checks that you did not write. Close current checking and savings accounts and obtain new account numbers and passwords.

## Legal and Government Agencies

- Report the crime and file a police report. Request a copy of the report and keep the phone number of your investigator handy. A complaint can also be filed with the Federal Trade Commission, although they do not assist with individual cases.
- Notify the US Postal Inspection Service if your mail was stolen or your address was used fraudulently.

## Credit Reporting Bureaus

- Check your credit reports from all three bureaus, Equifax, Experian, and TransUnion. Dispute any fraudulent items – this can be done by submitting a form on-line or mailing a letter to the credit bureaus.
- Even if the fraudulent information hasn't yet appeared on your reports, be proactive and report the crime to credit bureaus now. It is a good idea to have a fraud alert placed on your credit reports. When someone applies for credit under your name, the creditor must verify that the person applying is you. The initial fraud alert only lasts 90 days. However, if you file a police report, you can extend the alert to seven years.

## Action Log

Since you will be communicating with a lot of people and have many tasks to complete, use our Identity Theft Action Log to keep track of your efforts. Keep copies of all letters you send and receive, file paperwork promptly, and store everything in a safe and accessible place.

To download the Identity Theft Action Log (PDF format) log onto [www.cccssf.org/idtheft](http://www.cccssf.org/idtheft) and select "Download Action Log" from the left-side menu. Copies may also be obtained by calling CCCS at 800-777-7526.

## Helpful Resources

### Equifax

To order a credit report call: (800) 685-1111

To report fraud call: (888) 766-0008

[www.equifax.com](http://www.equifax.com)

### Experian

(888) 397-3742

[www.experian.com](http://www.experian.com)

### TransUnion

To order a credit report call: (800) 888-4213

To report fraud call: (800) 680-7289

[www.transunion.com](http://www.transunion.com)

### Annual Credit Report Request Service

(877) 322-8228

[www.annualcreditreport.com](http://www.annualcreditreport.com)

### U.S. Federal Trade Commission

(877) 438-4338

[www.ftc.gov](http://www.ftc.gov)

Download FTC's Identity Theft Victim's Complaint and Affidavit:

[www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf](http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf)

### U.S. Postal Inspection Service

(877) 876-2455

<http://postalinspectors.uspis.gov>