

Identity Theft



By Detective John Alvarez
Corona Police Department
High Technology Crimes Unit

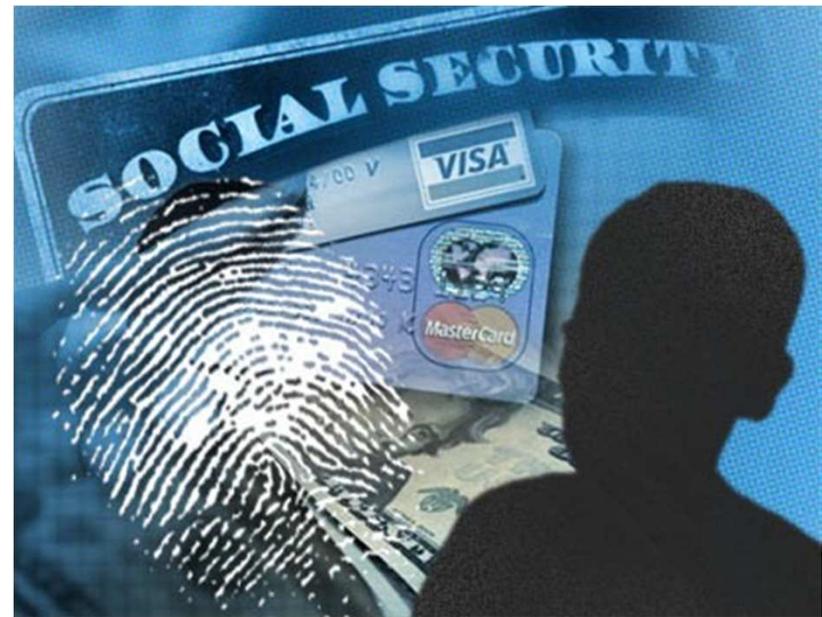
Legal definition of identity theft

- California Penal Code 530.5(a) defines Identity Theft:

Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person, is guilty of a public offense, and upon conviction therefore, shall be punished by a fine, by imprisonment in a county jail not to exceed one year, or by both a fine and imprisonment, or by imprisonment in the state prison.

The simple definition

- Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.



How common is identity theft?

- Estimates vary, but some studies estimate that nearly **13 million** Americans had their identities stolen in 2010.



Why is identity theft so popular?

- It's an easy crime with little or no victim contact.
- Less risk and more payoff. Why use a gun to rob a liquor store to only get a couple hundred dollars and risk significant jail time? A financial crime will most likely yield more money with significantly less risk of a long prison sentence.
- If done properly, it is easy to not get caught.

How do criminals steal your identity?

- **“Dumpster Diving”** – Criminals rummage through trash under the guise of recycling while all the while looking for paperwork with your personal information.



How do criminals steal your identity?

- **Skimming** – Credit and debit card information is copied by using a special storage device when processing your card.



How do criminals steal your identity?

- Infecting your computer with viruses and spyware.
 - Make sure to have up-to-date antivirus and spyware protection.
 - Install all updates (Windows and installed programs).
 - Know the basics of internet safety.

How do criminals steal your identity?

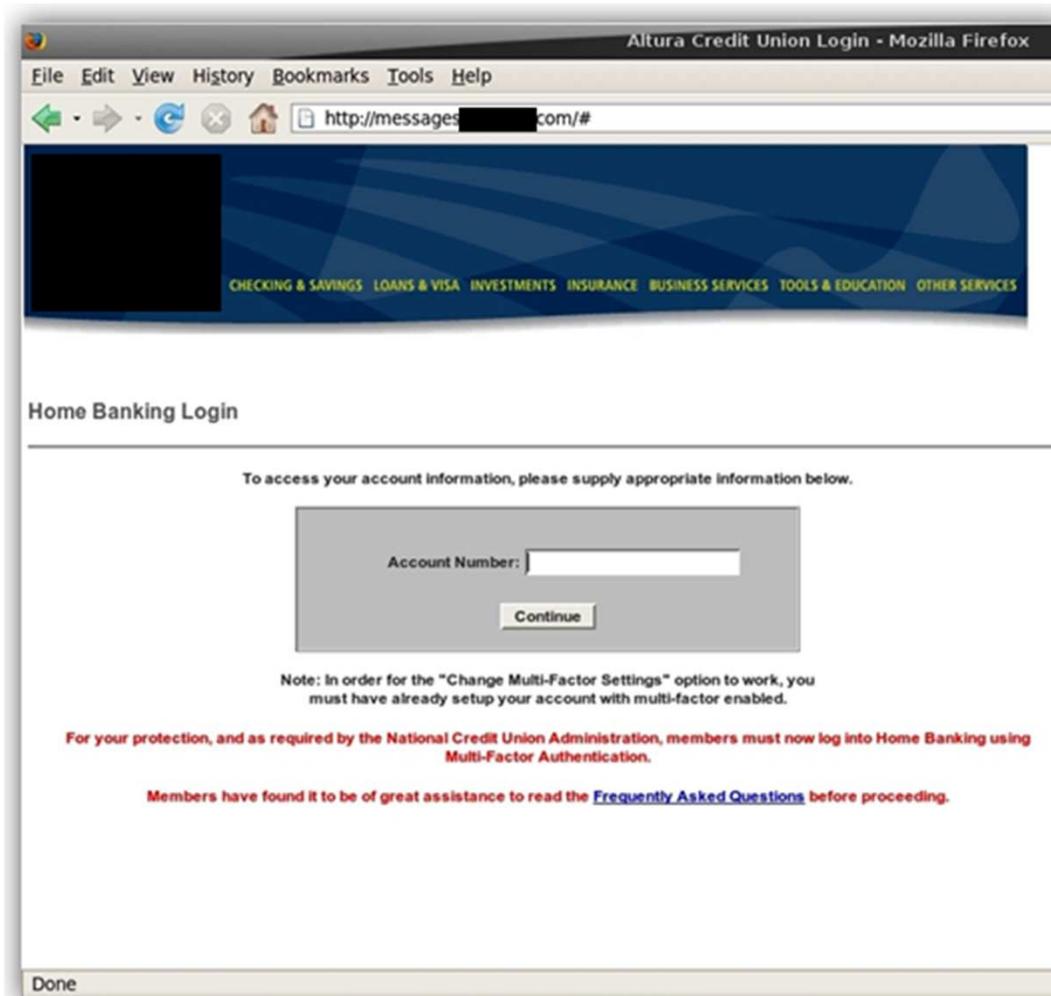
- **“Phishing”** – Thieves pretend to be financial institutions or other companies and send spam to try and fool you into revealing your personal information.



Credit union phishing scam

- An email phishing scam alerted recipients to a “problem” with their account and it stated they would not be able to log in until they verified information. Victims were provided an official looking link in the email that took them to the following website:

Credit union phishing scam



Credit union phishing scam

- Once a victim entered their account number, the next web page asked a few alarming questions...

Full Name	<input type="text"/>
E-mail address	<input type="text"/>
Zip Code	<input type="text"/>
16 Digits Debit Card Number	<input type="text"/>
Debit Card Exp. Date	Month <input type="text"/> Year <input type="text"/>
Debit Card Cvv2	<input type="text"/>
4 Digits Debit Card ATM PIN (REMEMBER! This is not the password you use to login)	<input type="text"/> Personal Identification Number you use at ATM machine
Verify Debit Card ATM PIN	<input type="text"/>

Credit union phishing scam

- After entering extremely sensitive account information, victims were sent to the real credit union web page.
- Many victims likely had no idea what had happened because they were able to log in.

Other ways criminals steal your identity?

- **Changing your address** – They divert your billing statements to another location by completing a change of address form.
- **Old-fashioned theft** – They steal wallets and purses; U.S. mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.

Other ways criminals steal your identity?

- **Pretexting/social engineering** – They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources. Thieves will call companies and convince employees that they are you and get whatever they might need.

What do thieves do with a stolen identity?

- Anything you would do with your good name!
- Open new credit card accounts in your name.
- Utilities fraud (electricity, heating, cable TV, home telephone, cell phone, etc.).
- Create counterfeit checks using your name and/or account number.
- Clone your ATM or debit card and make electronic withdrawals your name.

What do thieves do with a stolen identity?

- Take out a loan in your name.
- Use your name and Social Security number to get government benefits.
- Get a job using your Social Security number.
- Rent a house or apartment.
- Sell your information to other criminals.

What do thieves do with a stolen identity?

- Give police your personal information when committing a crime. If they do not show up for court, an arrest warrant is issued in your name.



Resolve a false criminal record

- Register as a victim of identity theft with the Department of Justice.
- You will need to complete a packet and include the following:
 - Court Order verifying victim status (contact your nearest court for the applicable order)
 - Application for Registration as Victim form
 - Applicant fingerprint submission form

Resolve a false criminal record

- You will probably need to carry proof of the false record for quite a long time.
- Visit the Office of the Attorney General website for instructions in case you become a victim of this crime:

<http://www.ag.ca.gov/idtheft/general.htm>



How to protect yourself

-  Use a cross-cut shredder and shred anything with your name on it – even if it is just your name and address.
- Consider using a standard ATM card in place of a Visa Check Card.
- Watch for card skimmers when using any card reader or ATM. Skimmers have been placed on all kinds of legitimate machines.

How to protect yourself

- Closely monitor your bank account and credit reports to catch suspicious activity early.
- Consider private identity theft protection companies.
- Protect your mail. Consider using a locking mailbox for mail delivered to your home, dropping your outgoing mail at the post office or in a drop box just before a pickup time, or getting a post office box.

How to protect yourself ~ tech

- Do not respond to any email or click on any hyperlink from a bank or creditor alerting you to a problem with your account or asking for your personal information.
 - If you get an email that is supposedly from your bank, check with the bank directly. Financial institutions generally will not request information via email and they will post alerts about scams on their website.

How to protect yourself ~ tech

- Securely wipe hard drives or flash drives when donating or disposing of old computers. Merely formatting a hard drive or flash media will not make the information unrecoverable. Wiping overwrites data with random information and makes it [nearly] impossible to recover.



How to protect yourself ~ tech

- Use a credit card with online fraud protection for online purchases.
- Try and do some research about companies that you will be dealing with online.
- Use a “clean” computer for online banking and financial transactions. A computer that is infected with viruses and spyware may be sending your account numbers, usernames, passwords, and other information to criminals.



How to protect yourself ~ tech

- Use strong passwords.
- Do not reveal too much on social networking sites (Facebook, Myspace, etc.). Keep your information private. Some people disclose enough about themselves that a criminal may use this information for fraud.

What you cannot prevent...

- Theft of your information from third parties.
- Loss of your information. **Millions** of confidential records are lost by corporations every year. Just look for articles – it is alarming how often it occurs.
- Compromised websites – many companies have their servers hacked and information stolen.
- Use of your information by friends or family.

Lost or stolen?

- "On February 27, 2009, BNY Mellon was transferring a load of computer tapes containing information including names, addresses, dates of birth and Social Security numbers, when it lost a tape carrying data on about **4.5 million people.**"

Lost or stolen?

The Internet home of: FORTUNE Money FORTUNE SMALL BUSINESS [Subscribe to](#)

CNNMoney.com

[GET QUOTES](#) SYMBOL LOOK-UP [SEARCH](#) Entire Site

[HOME](#) [NEWS](#) [MARKETS](#) [MY PORTFOLIO](#) [TECHNOLOGY](#) [JOBS](#) [PERSONAL FINANCE](#) [LUXURY](#) [REAL ESTATE](#)

[NEWS](#) > [Fortune 500](#)

[SAVE](#) | [EMAIL](#) | [PRINT](#) | [RSS](#)

Info on 3.9M Citigroup customers lost

Computer tapes with information about consumer lending lost by UPS in transit to credit bureau.

June 6, 2005: 5:13 PM EDT

NEW YORK (CNN/Money) - Citigroup said Monday that personal information on 3.9 million consumer lending customers of its CitiFinancial subsidiary was lost by UPS while in transit to a credit bureau -- the biggest breach of customer or employee data reported so far.

Citigroup, the nation's biggest financial services company, said that UPS lost the tapes while shipping them to a credit bureau in Texas.



Special Report
MISSION: SECURITY
Full coverage



Fortune 500
See more stories

How do you find out if your identity has been stolen?

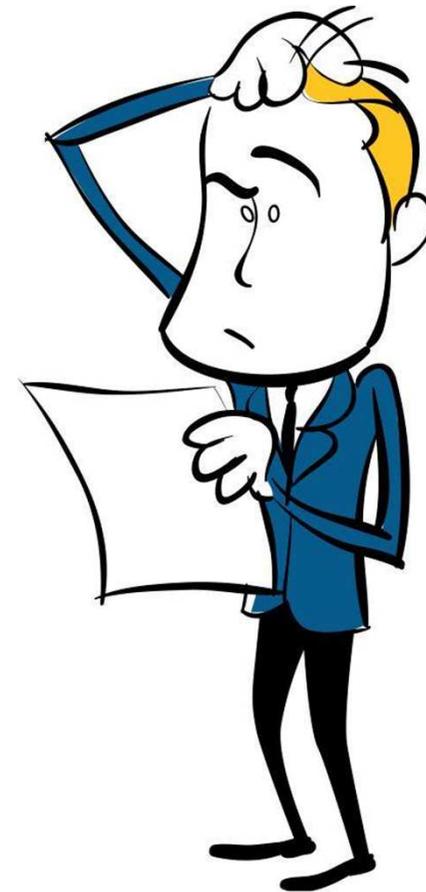
- Monitor your accounts and bank statements each month.
- Review your credit report on a regular basis. You may be able to limit the damage caused by identity theft if you catch it early.
- You may find out when bill collection agencies contact you for overdue debts you never incurred.

How do you find out if your identity has been stolen?

- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.
- You may get a bill from the IRS for unpaid taxes.

When it's too late...

- No matter what you do or how careful you are, you may still end up a victim.



What do you do now?

- File a police report with the law enforcement agency in your jurisdiction. *Have evidence of the crime ready for law enforcement (collection notice, bank statement, etc.) or the agency may not take a report.
- Collect as much evidence as possible on your own because financial institutions are not very cooperative with law enforcement without a warrant.

What do you do now?

- Besides filing a report with law enforcement, make a report with the Federal Trade Commission (FTC).
- You can use their [online complaint form](#) or call the Identity Theft Hotline: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.
- By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves.

What do you do now?

- Contact all three creditor reporting agencies and request a “**security freeze.**”
- Security freezes are designed to prevent a credit reporting company from releasing your credit report without your consent.
- Controls who is allowed access your personal and financial information.
- May delay, interfere with or prohibit the timely approval of an application you make regarding a new loan, credit, etc.

What do you do now?

- You will be issued a PIN or password for your account.
- You will need to release the freeze when you are applying for credit.
- If the freeze is not released, credit will not be opened in your name.

What do you do now?

- Set up a folder to keep a detailed history of this crime.
- Review your credit reports on a regular basis.
- Keep a log of all your contacts and make copies of all documents.

What will a police report do for you?

- Even if the criminal is not caught, a report can do a few things:
- A police report may be needed to get copies of the thief's application, as well as transaction information from companies that dealt with the thief (though by law you are entitled to a credit application you supposedly completed).
- To get this information, you may need to submit a request in writing, accompanied by the police report, to the address specified by the company for this purpose. Example forms are available on the Corona Police Department web site.

What will a police report do for you?

- Identity theft reports can prevent a company from continuing to try to collect debts that result from identity theft, or selling them to others for collection.
- An identity theft report is needed to place an extended fraud alert on your credit report.

How long can the effects of identity theft last?

- It is difficult to predict how long the effects of identity theft may linger because of many factors:
 - The type of theft.
 - Whether the thief sold or passed your information to other thieves.
 - Whether the thief is caught.
 - Other factors related to correcting your credit report.

What can you do to help fight identity theft?

- Be aware of how information is stolen and what you can do to protect yours.
- Monitor your personal information to uncover any problems quickly.
- Know what to do when you suspect your identity has been stolen.

Free annual credit reports

- Review your credit report annually, at the very least.
- You are entitled to one free credit report each year from each of the three nationwide consumer reporting companies. To order, visit annualcreditreport.com or call 1-877-322-8228.
- Do not contact the three nationwide consumer reporting companies individually. They are providing free annual credit reports only through annualcreditreport.com.

The not so free “FreeCreditReport.com”

- Only one website is authorized to provide your free annual credit report – annualcreditreport.com. Other websites that claim to offer *free credit reports*, *free credit scores*, or *free credit monitoring* are not part of the legally mandated free annual credit report program.

Source: <http://www.ftc.gov/bcp/conline/pubs/credit/freereports.shtm>

Resources

Office of the Attorney General website:

<http://www.ag.ca.gov/idtheft/general.htm>

Security Freeze

Experian: http://www.experian.com/consumer/security_freeze.html

Equifax: http://www.equifax.com/cs/Satellite?c=EFX_ContentRoot&cid=1165203975981&pagename=5-1%2F5-1_Layout

TransUnion:

<http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page>

Federal Trade Commission links:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/filing-a-report.html>

<http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idto5.shtm>

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>

Opt out of credit offers:

<https://www.optoutprescreen.com/?rf=t>

California Legal Codes:

<http://www.leginfo.ca.gov/calaw.html>

Resources

Free annual credit report:

<https://www.annualcreditreport.com/cra/index.jsp>

Credit bureaus:

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790