Identity Theft & Identity Fraud

By Kevin Sullivan
Table of Contents

What is Identity Theft? ........................................................................................................................................ 3
What is Identity Fraud? .................................................................................................................................... 4
How is Personal Information Stolen? ............................................................................................................ 5
How Your Personal Information is Used ..................................................................................................... 6
Minimizing Your Risks / Prevention Tips ..................................................................................................... 7
What To Do If You Are Victimized ............................................................................................................... 10
About Kevin .................................................................................................................................................. 12
Bibliography .................................................................................................................................................. 12
What is Identity Theft?

Identity theft is a crime when someone knowingly and unlawfully uses another person’s personal identifying information in a way that involves fraud or deception. The most common type of personal information obtained by identity thieves are items such as, name, address, date of birth, Social Security number and Drivers License numbers. These crimes usually are committed for the purpose of economic gain.

Currently, identity theft is the fastest growing crime in the United States. A distant second is Internet Fraud. The General Accounting Office estimates that as many as 750,000 Americans are victims of identity theft each year. That number might even be low due to identity theft being under-reported as many victims elect not to report the event to the police, and/or numerous subjects are unaware that they’ve even been victimized.

There are four types of identity thefts:

1. **Identity Theft for Financial Gain** - The victims name and Social Security number is used to apply for credit, loans and/or services.
2. **Identity Theft Criminal Impersonation** - The victims name and/or other identifying information is used by a subject when questioned and/or arrested by law enforcement. Subsequently, when the subject is a no show in court, an arrest warrant will be issued in your name.
3. **Cloning an Identity** - The victims information is used to duplicate a financial history. The subject takes the victims identity and lives as the victim, using and abusing the victims good credit.
4. **Identity Theft for Businesses** – What can be done to an individual can be done on a business or corporate level. Accounts are established in the name of a legitimate established business.
What is Identity Fraud?

Identity fraud, which includes identity theft, is the use of false identifying information, false or fraudulent documents, or a stolen identity in the commission of a crime. Typically it begins with a breeder document, which was created from fictitious or stolen personal information. The breeder document (drivers license/birth certificate) is used to create other supplemental documents. The end result is the genesis of a new identity, one that could be the doorway to criminal activity and/or terrorism. Identity fraud has an expanded definition as it refers to the deceptive use of any identity, either real or fabricated, while identity theft is restricted to the theft of an actual person’s identity.

An even larger and much more daunting issue for law enforcement is the identity that is created from fraudulent breeder documents. This is of grave concern as an identity thief could potentially go for years without being discovered. Members of structured criminal organizations and/or terrorists would want to make use out of this situation.
How is Personal Information Stolen?

Identity thieves will use a plethora of techniques to obtain access to your personal information. Some of those are:

- From Businesses
  - Stealing records from the employer
  - Paying off a corrupt employee
  - Hacking into the companies computers
  - Dumpster diving (rummaging through the trash)
  - Obtaining credit reports by exploiting a legitimate companies use of a credit report through a dishonest employee (e.g. car dealers or loan companies)
  - Skimming your Credit or Debit Card

- From You
  - Pickpocket your wallet (often times even returning your wallet after having skimmed your credit card and copied your personal identifying information).
  - Obtain your info right from your home. (e.g. an unscrupulous delivery person or someone who has access to your home.
  - Contact you by phone, mail or e-mail, and mislead you into believing that they are someone else who needs your info (e.g. utility company, police, contest winner)
  - Remove the mail from your mailbox. All your bills or statements will have your name and account number and some even have your Social Security number and phone.
  - A post office change of address form is submitted attempting to divert your mail to another location.
How Your Personal Information is Used

There are almost as many ways for a criminal to use a victim’s personal information as there are ways to obtain it. Some of the ways identity thieves will use a victim’s information is as follows:

- Apply for a credit card
- Apply for a loan
- Apply for a mortgage
- Purchase a vehicle
- Purchase a cellular telephone
- Apply for a checking account
- Place utility bills in your name
- File for bankruptcy
- Provide your name to the Police during an arrest

The concept for the identity thief is to have all bills and/or statements sent to an address other than the victim’s legitimate address. While the identity thief is charging merchandise on a victim’s credit card, the victim is unaware of the activity. Once a victim reviews his statement, he will realize that something is wrong and contact the financial institution that issued that particular credit card. By keeping the statement away from the victim, the identity thief has more time to make more purchases.

For some items, a victim may never see a statement, nor even be aware to look for one. For example, if an identity thief purchases a vehicle using a victim’s personal information and alternate address, the victim would never even realize that such an event has taken place. That is until some day when a representative from the car loan company contacts the victim inquiring about the late payments on his car. In many instances, the victim is not alerted to the events until the identity thief has inflicted significant harm to the victim’s credit and reputation.
Minimizing Your Risks / Prevention Tips

There are many actions that can be implemented to reduce the risk of becoming an identity theft victim however, even if you have been very careful about protecting your personal information, you can still be the victim of an identity theft. High tech solutions are constantly in development and hopefully someday all risk associated with your identity will be removed. The following are suggestions for minimizing your risk:

- Obtain a copy of your credit report. This report contains information about any credit accounts that have been opened in your name. Additionally, it contains information about your loans, how much and how frequently you pay, and if you have ever applied for bankruptcy. Most merchants and loan companies use a mathematical system to score your credit report. The higher the score the better and more likely you are to gain approval on a loan, or obtain a better credit rate. Poor scores can subject you to non-approval of loans including mortgages. A victim of identity theft may have a very low score. Further, check with each credit reporting company on a regular basis, at least once year.
  - To obtain a copy of your credit report you should contact the credit bureaus. (These phone numbers are not for reporting fraud – please refer to section on What to do if You Are a Victim for the appropriate phone numbers)
    - Equifax - [www.equifax.com](http://www.equifax.com)
      - Order a report – 1-800-685-1111
    - Experian – [www.experian.com](http://www.experian.com)
      - Order a report – 1-888-397-3742
    - TransUnion – [www.transunion.com](http://www.transunion.com)
      - Order a report – 1-800-888-4213

- Secure personal information in your home. If you are having outside workers come to your house or if you have roommates, make an effort to secure all bills, statements, checkbooks, credit cards and any other sort of financial information.
• Do not give out any personal information to anyone on the phone, mail, e-mail, or Internet unless you are the one who initiated the contact. Identity thieves may pose as bankers, police, utility companies etc. Ask for their name, agency, location and main number. You then should call 411 or go to the company’s web site to get the main number to verify. You can call the main number and then ask for the person by name.

• Shred your trash. Identity thieves will go through your trash, hence the term, “dumpster diving.” If possible purchase a shedder and make use of it for all your discarded mail.

• Deposit outgoing mail in official post office collection boxes. When you put your mail in the box at the end of your driveway and turn up the flag, you are just announcing to identity thieves that there is something in your box just waiting to be intercepted. Further, if you are not home everyday to promptly remove incoming mail from your mailbox, then consider using a secured post office box.

• Review all statements each month for accuracy. Understand the billing cycles and inquire if a bill does not arrive on time.

• Don’t give out your Social Security Number unless absolutely required. Don’t carry your Social Security Card, or any card that uses your Social Security number (health insurance) with you on a routine basis.

• Skimming – This can occur at merchants that normally take your credit card from you to swipe (restaurants/gas stations). An unscrupulous individual working at that merchant may swipe your card twice. Once into the legitimate system and once into an identity thief’s system. All the information on the magnetic stripe on the back of your card is copied and a fraudulent, duplicate credit card is created. Don’t let your card out of your sight.

• Computers
- Make use of a firewall program. This is similar to locking your front door. Without locking your door, criminals may be able to walk in and take what they want.

- Always use a secure browser when purchasing items over the Internet. This encrypts your personal information so if it is hijacked along the way, it will be in code.

- Stay away from using an automatic log in which saves your password. If someone were to get access to your system, they would have your password.

- When you sell or get rid of your computer, use a utility program that cleans and erases your hard drive so that personal information will not be left on the machine.

- Phishing Scams - Identity thieves use e-mail to link a consumer to a phony Web site that looks and appears to be a legitimate site for a company (government or private). Next the victim is asked to confirm his account information by entering it into an official looking form.
What To Do If You Are Victimized

Identity theft victims often feel confused, frustrated and overwhelmed. Identity theft is an emotionally draining and repetitive crime. It may feel like the battle will never end as more notices arrive from various creditors. The true victim feels as if he is a convicted felon and must prove his innocence to the banks, merchants, police etc. Fortunately, in an ironic twist, because identity theft has been so prevalent, more and more financial institutions are now comprehending the damage done by a victim's destroyed credit and adapting policies to reflect an understanding of the situation.

If you believe that you are the victim of an identity theft then several actions should be completed as soon as possible. Additionally, maintain a log of all your contacts and correspondence. The following steps should be observed:

1. Contact the fraud departments of any one of the three major credit bureaus. (The three major credit bureaus maintain a shared database for fraud alerts). Advise them that you believe that you are a victim of an identity theft and are requesting a fraud alert be placed on your credit report.
   a) Request that any and all creditors contact you before opening any new accounts or altering existing accounts.
   b) Request that a credit report from each of the three major credit bureaus be sent to you. (This will be done free of charge). Review your report for any unknown accounts and/or unexplained debts.

   ▪ Equifax - [www.equifax.com](http://www.equifax.com)
     o To report fraud – 1-800-525-6285
   ▪ Experian - [www.experian.com](http://www.experian.com)
     o To report fraud – 1-888-Experian
   ▪ TransUnion – [www.transunion.com](http://www.transunion.com)
     o To report fraud – 1-800-680-7289

2.
a) Contact all of the creditors for any account that is fictitious or has been altered. After calling the creditors, you should follow up with a letter (registered mail) as that is the method that the consumer protection procedure law specifies.

b) Report to the Social Security Administration if you believe someone is using your Social Security Number at another job.

   - SSA Fraud Hotline – 1-800-269-0271

c) If your checks have been misused, close the account and ask the bank to notify the appropriate check verification service. Additionally, you should contact the major check verification organizations.

   - Telecheck – 1-800-710-9898
   - Certegy, Inc. – 1-800-437-5120
   - International Check Services – 1-800-631-9656
   - SCAN – 1-800-262-7771
   - CrossCheck – 1-707-586-0431
   - Equifax Check Systems – 1-800-437-5120

3. File a report with your local police or the police in the area where the identity theft occurred. Maintain a copy of the police report (or at least the police case number) as you may be required to show proof of the report to your creditors.

4. File a complaint with the F.T.C. (Federal Trade Commission). This information is entered into an FTC database, which is accessible only to law enforcement agencies that are pursuing leads in various criminal investigations. File an ID Theft Affidavit. This form is used to report information about the crime to many different organizations. For a copy of the affidavit, view the ID Theft website.

   - www.consumer.gov/idtheft
   - FTC’s Identity Theft Hotline – 1-877-IDTheft

Other agencies that may be contacted depending upon the individual case:

- FBI
- US Secret Service
- US Postal Inspection Service
- Social Security Administration
• Internal Revenue Service
• Securities Exchange Commission

About Kevin

Kevin Sullivan, MS, MMBA, CAMS, was an Investigator with the New York State Police, and he coordinated NY state investigations at the New York HIFCA El Dorado Intelligence Center. Sullivan is co-chair of the NY chapter of ACAMS.

Bibliography

“Identity Theft.” ID Theft Resource Center.com. 10 Jan 2005

“Identity Theft Resources.” Privacy Rights Clearinghouse 4 Jan 2005

“ID Theft.” Federal Trade Commission. 29-Dec 2004
30-Dec 2004<http://www.consumer.gov/idtheft

“Identity Theft Prevention and Survival.” Identity Theft.org 30-Dec 2004
30-Dec 2004<http://identitytheft.org/index.htm

“Identity Theft is America’s Fastest Growing Crime” USPS.gov 3-Jan 2005
3-Jan 2005<http://www.usps.com/postalinspectors/idthft_ncpw.htm

“Identity Theft and Identity Fraud” USDOJ.gov 10-Jan 2005

“Don’t Let This Happen to You” FBI.gov 4-Jan 2005
4-Jan 2005<http://www.fbi.gov/page2/oct04/preventiidt102104.htm

“Access Device Fraud” treas.gov/usss 10-Jan 2005

“Identity Theft” SSA.gov 9-Jan 2005

“The Use of Technology to Combat ID Theft” Treas.gov 20-Feb 2005