THE Blakeley GROUP

Identity Theft 2016:
An Ounce of Prevention is Worth a Pound of Cure

Introduction

Identity theft is when someone steals your personal information and uses it without your permission. It is serious crime that can really make a mess of your finances your credit history, and your life.

Identity theft can happen to anybody; victims include a former chairman of the Joint Chiefs of Staff, the head of a large hedge fund, celebrities, corporate CEOs, and even the chairman of the Federal Trade Commission.[1] A study conducted by Experian in 2010 identified *affluent suburban households* as the most at-risk demographic for identity theft.[2]

In 2014, a number of high-profile hacking incidents of companies such as Target, Michael's, JPMorgan Chase, Home Depot, Staples, Sony Pictures, and Anthem Health Insurance have brought the issue of identity theft protection to the forefront of the business and personal security world. The perpetrators of these hacks obtained employee information, customer credit card information, and social security numbers.

The Blakeley Group does not want you to become a victim of identity theft.

This paper is intended to serve as a supplemental information resource regarding identity theft. It is a comprehensive guide on protection, detection, and elimination of the threat of identity theft. This paper contains analytical information on the dimensions, prevalence, and extent of identity theft, suggests methods that can be used to minimize the risk of becoming a victim of this crime, and includes steps to take that may potentially limit the damage caused if victimized by it. Found at the end is a list of key resources and further reading on the topic.

The Cost of Identity Theft

Identity theft is a significant and pervasive threat. Javelin Strategy and Research estimates that in 2013 more than 13.1 million Americans had their personal information used for illegal financial gain.[3] Identity theft costs victims significantly in terms of time, money and, most importantly, their good name and credit status. Innocent casualties who have compromised credit ratings may be unable to get a new job, buy a new home, or borrow money to finance a business.

Identity theft has topped the Federal Trade Commission's annual list of consumer complaints for the past 15 years, representing 13% of all complaints in 2014.[4] The personal and financial impact is considerable. The Javelin Strategy and Research study noted earlier puts the total cost of identity theft at $18 billion in 2013, significantly less than the all-time high of $48 billion recorded in 2004. However, the decrease in total cost was accompanied by an increase in the number of people affected by almost half a million. This increase in identity theft occurrences

accompanied by a dramatic drop in out-of-pocket costs may reflect the increasing prevalence of less severe types of fraud.[3]

Sources of Theft

Why is identity theft the crime most often reported to the FTC? The unfortunate answer lies in both the ease of acquiring personal and financial information plus the low probability of being caught.

The key components of an individual's identity are at risk not only from his or her own actions, such as losing a wallet or purse, but also by the actions of others who have their information legitimately. Countless merchants, employers, data brokerage companies, payment processing agencies, card networks and other businesses who have vital information may be hacked by computer thieves, conned or scammed by outsiders or employees, or simply lose it by mismanagement. Over 781 breaches or losses of information by companies in 2015 in the United States exposed almost 169 million identities to risk.[6]

Sometimes the perpetrator is a person known to the victim, such as a relative or roommate. Other thieves represent a broad cross-section of criminals such as members of gangs or other organized crime enterprises and drug addicts. Some even work for the government, and steal information while on the job.

A survey of underground hacker networks conducted in 2014 by Dell SecureWorks found that these markets were "booming with counterfeit documents, dossiers of personal information, and customer satisfaction guarantees." Their findings include:[5]

- Anyone can purchase a scan of a social security card, name, and address for $250. For another $100, the hacker will include a utility bill for additional identity verification.
- United States-based driver's licenses can cost from $100 to $150 each.
- On average, stolen credit cards can sell for $25 apiece. The cost is more for premium cards, less for international cards. The price per card is less when bought in bulk. When a successful identity thief can make thousands of dollars from just one card, this becomes an extremely profitable and relatively low-risk venture.

Common Theft Techniques

How do identity thieves acquire information? According to Epsilon Data Management, common tactics used to commit fraud and identity theft include:[7]

- **Email Phishing** - Phishing emails look a lot like a legitimate email from a reputable company, or even a government agency, but actually originate from a criminal. The email usually directs you to a website that also looks legitimate where you are asked for sensitive personal information, such as your social security or account number. Typically, the goal of email phishing is to have the recipient provide sensitive personal information so the perpetrator can commit further fraud.
  - If you receive a suspicious email, do not open it and do not click on any links in the email if you have opened it. Contact the sender and ask if they sent you the email.

Never supply financial account information or your social security number in an email or in response to an email you have received.

- **Telephone Scams** - Telephone scammers contact you by telephone and request that you provide some form of sensitive personal information, such as your account or payment information, to verify your identity or to sign you up for a new product. Often they will have a reason for needing your information immediately. For instance, someone posing as a PG&E employee will claim your power is going to be shut off that day unless you update your payment information. Any company you do business with that already has your personal information will not request the same information again if they contact you to discuss your account, and they certainly won't handle payment information over the phone; although they may ask questions that may contain a portion of the information to verify your identity.
  - If you have any reservations about the request, it is always best to contact the business or agency by phone using the contact information you have already been provided instead of any contact information the person on the phone may provide.
- **Stealing** - A thief can obtain your credit card number or other sensitive information by simply stealing it. For example, a thief may steal the credit card number by personally handling the card when you make a purchase, or may steal your wallet or purse and use your financial cards. Also, some criminals may steal mail, which could contain bank statements, bills and other documents with your sensitive personal information.
  - If you are going to be away from home for an extended period of time, have the Post Office hold your mail or have a trusted friend or neighbor collect it for you.
  - Don't carry your social security card or other unnecessary personal documents in your purse or wallet if they are not needed. Always be careful when giving your credit and debit cards to someone to make a purchase.
  - Know how to immediately freeze or otherwise halt any credit or debit cards that are lost or stolen and report the incident to your bank.
- **Skimming** - Criminals also use copying technology on point-of-sale terminals and ATM terminals to obtain credit card numbers. Be careful when swiping a credit or debit card for a purchase to ensure that no additional technology is attached to the machine. If you are unsure or hesitant, ask that the cashier swipe your card on the register, or pay with cash or check.
- **RFID (Radio Frequency Identification) Skimming** is a form of digital theft, where the thief uses a cheap RFID reader device to download the information off RFID chips embedded in some credit and debit cards. These reader devices are small and work at a distance, making it easy for the thief to steal information while remaining hidden or inconspicuous. Consider investing in an RFID blocking wallet or RFID blocking card sleeves.
- **Dumpster Diving** - It's common for criminals to search through dumpsters looking for bills or other papers with your sensitive personal information on it. When someone does not properly dispose of paper documents with information such as credit card numbers or social security numbers on them, a criminal is able to take that information and commit fraud or identity theft. Make sure to thoroughly shred documents with sensitive information and any blank applications that come with credit card offers or other mail. Consider shredding anything you wouldn't want to fall into dubious hands.

Types of Fraud

▪ **Account Takeover** – The two most common ways for criminals to commit account takeover fraud is to add their name as a registered user on an account, or change the address associated with the account.
▪ **New Account Fraud** – New account fraud is the most costly to victims. Fraudulent opening of non-bank accounts, such as health club or utility subscriptions, is becoming more common and is more difficult to detect. Consumers may not be able to detect this type of fraud by checking credit reports, and should carefully examine financial statements and consider utilizing a service that monitors public records.
▪ **"Friendly Fraud"** – This type of fraud accounted for over 30% of new account fraud for which the cause was known. In cases of friendly fraud, new account fraud was more than twice as common as existing account fraud. The minority of thieves acquired identities online by such means as spyware (malicious programs that sit on a computer and collect pertinent keystrokes) and "phishing" (sending bogus e-mails that look like they come from legitimate companies in order to acquire "updated" information).
▪ **Real Estate Fraud** – Real estate fraud is any illegal activity affecting a home. This includes stealing your identity to purchase a house or applying for a home loan without your knowledge, forging your signature on a deed or other document, and tricking you into paying for services that do not help you or that you do not need. Be careful when doing business with people who you've never met face-to-face, and avoid doing business with strangers you meet on the internet or at coffee shops. Con artists may approach you at church, temple, or other typical meeting sites. Don't go to coffee shops or restaurants to complete deals, as legitimate companies have real offices. Do your homework; check the names of individuals and companies on the internet to see if there are complaints against them. Never pay for real estate deals in cash. If it sounds too good to be true, it probably is!
▪ **Medical Identity Theft** – If an identity thief gets medical treatment using your name the thief's medical information, such as blood type, test results, allergies or illnesses, can get into your medical file. Information about the thief can be added to your medical, health insurance, and payment records. The thief might deplete your health insurance benefits.

Future Trends

What trends in identity theft can consumers expect to see going forward? The Identity Theft Research Center predicts an increasing prevalence of:[8]

▪ **International Identity Theft** – Victims will increasingly find fraudulent credit or debit card charges from overseas transactions in Europe, Asia and Africa.
▪ **Social Engineering Theft** – Attempts to scam money and information using deception will become more sophisticated and more prevalent. The rapid growth of social media will lead to an increased frequency of crimes utilizing social networking sites, smart phones and mobile devices. Hackers continue to exploit online networks and use their sense of "community" to gather personally identifying information.
▪ **Cyber Theft** – Despite growing attention to appropriate defensive measures, cybercrime and hacking continue to increase. Cybercriminals will continue to hack into network servers and use skimmers at ATMs to steal card information.

▪ **Low Tech Theft** – Mail theft continues to be the top tactic for low tech identity thieves, followed by stolen wallets. Even as cyber security and other high tech safeguards have become increasingly important, U.S. Postal Inspectors break more identity theft cases than any other single law enforcement group.

As consumers become more aware and take positive steps, and as businesses are doing more to proactively prevent fraud from identity theft, many victims are discovering identity theft sooner. Nearly half of victims report uncovering the fraud within three months. However, 23% do not discover the crime for at least two years, indicating individuals can do more to proactively protect their identity.[9]

How to Minimize the Risk of Becoming a Victim

Identity protection means treating your personal information like your other valuables.

General Precautions

This list is compiled from various sources listed in the Important Resources section.

- ✓ Regularly review credit status and credit detail.
- ✓ Request free copies of your credit reports by visiting any of the major credit reporting companies' websites listed here (www.annualcreditreport.com, http://www.experian.com, http://www.equifax.com/CreditReportAssistance, http://www.transunion.com).
- ✓ Consider freezing access to your credit file if you live in one of the states that allow you to do so. Currently 35 states allow this, including: CA, OR, TX, NV, and NM. WA restricts credit freezes to victims of identity theft only.
- ✓ Do NOT carry a checkbook or your Social Security number. Only carry credit cards that you need and will use.
- ✓ Review activity statements for ALL accounts immediately when you receive them.
- ✓ Monitor online banking activities weekly.
- ✓ Never use debit cards to buy online or in questionable circumstances; credit cards have limited liability.
- ✓ Set up account alerts, such as mobile and email alerts, and place passwords on credit cards and other accounts that allow for such protection.
- ✓ Use secure passwords that are unpredictable combinations of upper- and lowercase letters and numbers. Do NOT use actual mother's maiden name, actual city of birth, middle name, pet's name, actual birth date, last digits of Social Security number, last digits of phone number, street address numbers, sequences of numbers such as 1, 2, 3, 4 or repeated numbers such as 5, 5, 5, 5. Also, be sure to change passwords periodically.
- ✓ Do NOT give out personal or financial information unless you initiate a phone call.
- ✓ Avoid being a victim of "phishing" by always confirming the source of an e-mail request for information and then responding by initiating a separate contact with the business in question. Think:
  - You have **NOT** won the lottery in Hong Kong, the Netherlands, Ghana or anywhere else. You didn't buy a ticket, did you?
  - A poor widow or Nigerian prince does **NOT** need your help to move money from their account to another place.

- The IRS is **NOT** electronically auditing you.
- The jury duty clerk **NEVER** calls for your Social Security number.
- Banks and credit card companies do **NOT** email you to verify your information.

✓ Do NOT list common personal identifiers on social media sites, such as mother's maiden name, pet's name, city of birth, etc.

✓ Do NOT give out your Social Security number (even just the last 4 digits) or other personal information unless absolutely necessary. When a Social Security number is requested always ask: Why is this needed? How will this information be secured? Can a different means of identification be used? What will happen if I do not provide my Social Security number?

✓ Be VERY careful with documents and your "hard" mail. Use a cross-cut shredder to destroy items that reveal personal and financial information or may be used to open a new, illegal account or give access to existing accounts, such as credit card notices and credit card checks.

✓ If possible, have mail delivered to a secure location and never put outbound mail in an unsecure mail box for collection. Always ask the US Postal Service to hold your mail if you are on vacation.

✓ Have new checks held at your bank's branch office for you to pick-up.

✓ Sign new credit cards you receive in the mail immediately.

✓ Opt out of free credit card offers sent by mail by calling 888-567-8688 or visiting (www.optoutprescreen.com). NOTE: you will be asked for your Social Security number to accomplish the opt-out.

✓ Secure personal information at your home. The incidences of identity theft by perpetrators who personally know the victim makes this very important!

✓ For personal computers: update virus protection software frequently; beware of file sharing; use a firewall program; use a secure browser; do not store financial information on a laptop unless files are password-protected; use a wipe program (like Darik's Boot and Nuke or HDShredder) to overwrite the hard drive of an old computer.

✓ Watch for unexpected bills regarding accounts you cannot recall establishing and be aware of bills that never come that should have already arrived in the mail.

✓ Use extreme caution when using an ATM; make sure you are not watched when entering your PIN and look for devices on the ATM that may imprint your ATM card.

Red Flags of Identity Theft

How do you know if someone has stolen your identity? Typical red flags include:

✗ Mistakes on your bank, credit card, or other account statements

✗ Mistakes on the explanation of medical benefits from your health plan

✗ Your regular bills and account statements don't arrive on time

✗ Bills or collection notices for products or services you never received

- Calls from debt collectors about debts that don't belong to you
- A notice from the IRS that someone used your Social Security Number
- Mail, email, or calls about accounts or job's in your child's name
- Unwarranted collection notices on your credit report
- Businesses turn down your checks
- You are turned down unexpectedly for a loan or job

Steps to Limit the Damage of Identity Theft

- **If you think someone has stolen your identity, *acting quickly* is the best way to limit the damage.**

1) Place a fraud alert with credit agencies, credit card companies and businesses [Credit Agencies: Experian (888-397-3742), Trans Union (800-680-7289) and Equifax (800-766-0008)] and freeze access to your credit records.
2) Review your current credit report carefully for unknown accounts and charges to existing accounts. Request to have errors removed as soon as possible, and keep a record of this.
3) Close targeted accounts as soon as possible and write to credit card companies and other businesses as a follow-up.
4) Change all passwords. As mentioned in the prior section, use secure passwords that are unpredictable combinations of upper- and lowercase letters and numbers whenever possible. Do NOT use actual mother's maiden name, city of birth, middle name, pet's name, birth date, last digits of Social Security number, the last digits of a phone number, street address numbers, and sequences of numbers or repeated numbers. Putting unique numbers at the beginning of a password is an easy way to make it more secure. Remember, you can use spaces in passwords!
5) Fill out the FTC Identity Theft Affidavit.
6) File a police report and send copies to credit agencies, creditors and companies involved in the theft. Mistakenly, many identity theft victims do not notify the police. Comply with any investigation to the best of your ability.
7) For all types of identity theft episodes, file a complaint with the FTC (www.ftc.gov/idtheft/).
8) Replace your Social Security numbers by calling the Social Security Administration at (800-772-1213).
9) Keep a file of all identity theft related paperwork and a chronicle of all conversations with credit agencies, creditors and companies involved in the theft.
10) Review your past methods to limit the risk of identity theft and adopt additional precautions in the future.

Important Resources

Identity Theft Affidavit:
http://www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf

Credit Bureaus

Equifax
Equifax Credit Information Services, Inc.
P.O. Box 740241
Atlanta, GA 30374
1.800.685.1111 for general inquiries
1.888.766.0008 to place a fraud alert on your credit report

Experian
1.888.397.3742 for consumer credit center
1.866.200.6020 to request a credit report by mail

TransUnion Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92834
1.877.322.8228 for your free credit report
1.800.680.7289 to report fraud

Websites

Federal Trade Commission (www.ftc.gov/credit), (www.ftc.gov/idtheft)

Identity Theft Resource Center (www.idtheftcenter.org)

National Consumers League's Fraud Center (www.fraud.org)

Free Credit Report Request Site (www.annualcreditreport.com)

US Postal Service – Postal Inspectors (https://postalinspectors.uspis.gov/)

LifeLock (http://www.lifelock.com)

Fight Identity Theft Initiative (www.fightidentitytheft.com)

National Crime prevention Council (www.ncpc.org)

US Justice Department – resources describing identity theft scams and how to avoid them (www.usdoj.gov/criminal/fraud/websites/idtheft.html)

The Consumers' Union reviews of states laws and services, including identity theft related laws and services (www.consumersunion.com)

Opt-Out of offers for credit or insurance (https://www.optoutprescreen.com/?rf=t)

How secure are your passwords? Test them at https://howsecureismypassword.net

Software Downloads

Password Corral - http://www.cygnusproductions.com/freeware/pc.asp

Darik's Boot and Nuke - http://www.dban.org/

HDShredder - http://www.miray.de/download/sat.hdshredder.html

FireSheep - http://codebutler.com/firesheep/
BlackSheep- http://research.zscaler.com/2010/11/blacksheep-tool-to-detect-firesheep.html

HotSpot Shield - http://www.anchorfree.com/

Books

Your Evil Twin: Behind the Identity Theft Epidemic by Bob Sullivan

From Victim to Victor: A step by step guide by Mari Frank

Stolen Lives: Identity Theft Prevention Made Simple by John D. Sileo

Taking Charge: What To Do If Your Identity Is Stolen pdf from the FTC website

Articles – Print and Online

"Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites," How-To Geek, January 2, 2014

"Firesheep, Blacksheep, and Protecting Your Wi-Fi Data," PCWorld, November 10, 2010

"How to Nab Identity Thieves," Barron's, May 17, 2010

"Understanding Identity Theft and Stopping the Crime," Computer and Internet Lawyer, March 2007

"US Identity Theft…" Dow Jones News Service, February 1, 2007

"NY, California More Likely Identity Theft Targets," Reuters News, February 14, 2007

"To Catch a Identity Thief," MSNBC, March 2007

About The Blakeley Group, Inc.

Founded by Dick Blakeley, we are an experienced team of financial advisors who invest the time required to understand each client's specific goals. Our highest priority is helping your family safeguard financial and real estate assets to minimize tax liabilities and best serve your long and short-term needs. Located in the heart of Silicon Valley, we serve high tech entrepreneurs requiring wealth building expertise and retiring professionals who need expertise and support through the complex retirement process.

Disclosure

The statements contained herein are the opinions of The Blakeley Group, Inc. All opinions and views constitute our judgments as of the date of writing and are subject to change at any time without notice. Hypothetical examples are shown for illustrative and educational purposes only. Information was obtained from third party sources, which we believe to be reliable but not guaranteed for accuracy or completeness. The information provided is not intended to be relied upon as investment advice or recommendations, does not constitute a solicitation to buy or sell securities and should not be considered specific legal, investment or tax advice. The information provided does not take into account the specific objectives, financial situation, or particular needs of any specific person.
The opinions expressed in these resources do not necessarily reflect the views of The Blakeley Group. The Blakeley Group assumes no liability for the content of any resource provided, including, without limitation, the accuracy, subject matter, quality or timeliness of the content. The fact that such resources have been provided does not constitute an endorsement, authorization, sponsorship by or affiliation with The Blakeley Group, Inc. with respect to any resource provided or its sponsor.
Investing entails risk including the possible loss of principal and there is no assurance that an investment will provide positive performance over any period of time.

[1] "The Scary New World of Identity Theft," Newsweek, July 4, 2005

[2] "Portrait of a Fraud Victim: Affluent Suburbans Most at Risk," Experian, Market Insight Snapshot, January 27, 2010

[3] "2014 Identity Fraud Report: Partnering with Law Enforcement," Javelin Strategy and Research, February 2014.

[4] "Consumers told it to the FTC: Top 10 complaints for 2014," FTC Consumer Information. February 27, 2015.

[5] "Underground Hacker Markets," Dell SecureWorks, December 2014. <http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf>

[6] "2015 Data Breach Stats," Identity Theft Resource Center, February 2016.

[7] "Fraud and Identity Theft," Epsilon, March 18, 2015.

[8] "ITRC Forecasts Black Ice Ahead in 2011," Identity Theft Resource Center

[9] "Identity Theft: The Aftermath 2009," Identity Theft Resource Center