

IDENTITY THEFT

THE FASTEST GROWING CRIME IN AMERICA





TABLE OF CONTENTS

01	WHAT IS IDENTITY THEFT?	02
02	HOW DOES IDENTITY THEFT HAPPEN?	03
03	WHO IS AT RISK FOR IDENTITY THEFT?	04
04	EMERGING AREAS OF IDENTITY THEFT	06
05	VICTIM STORIES	08
06	IF YOUR IDENTITY IS STOLEN	09
07	THE PROACTIVE SOLUTION	10



WHAT IS IDENTITY THEFT?



When a criminal assumes the identity of someone else for personal gain, it's called identity theft. This usually begins with a stolen piece of sensitive information, like a Social Security, bank account or medical insurance number. The crime affects 15 million Americans every year and can have serious and lasting consequences.¹ In addition to the financial impact, many victims spend years trying to restore their credibility and reputation.

FACTS

Identity theft is the #1 crime in America²

An identity is stolen every 2 seconds in the US³

3.6 million adults have lost money in phishing attacks⁴

It can take over 5,000 hours to recover from identity theft⁵

The average loss from identity theft is over \$3,000 per incident⁶

31% of identity theft subjects are victimized by friends or family⁷



HOW DOES IDENTITY THEFT HAPPEN?

It all starts when key personal information falls into the wrong hands, allowing criminals to impersonate you. Information, for example, that may be used to obtain a credit card or loan in your name. Of course, none of this happens by accident. Identity thieves employ countless tricks and methods to obtain the necessary materials. Worse yet, identity theft is a completely silent crime. No blaring car alarms. No broken kitchen windows. In fact, it takes most victims six months to realize their identity has been compromised.⁸

A FEW EXAMPLES OF HOW YOUR IDENTITY IS STOLEN

Dumpster Diving -Thieves sort through your garbage looking for personal information and documents, such as credit card applications. In many cases, mail is simply taken from an unlocked mailbox.

Phishing - Someone impersonates a company or important authority and emails you with an official looking request for important personal information, such as verifying your bank account number, Social Security number or passwords.

Basic Theft - A criminal obtains your personal information by stealing a wallet or sensitive files from your home such as bank statements, medical records and Social Security cards.

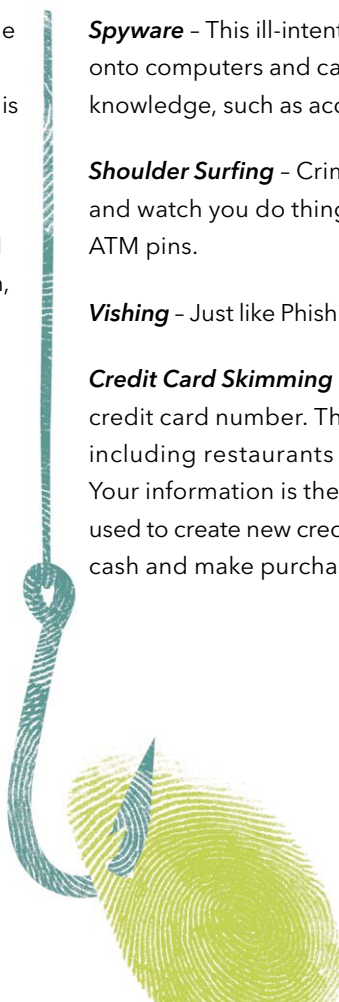
Hacking - Tech savvy thieves break into databases, computers and websites to retrieve your stored personal information. This can include everything from your name, address and birthday to highly sensitive data like Social Security numbers and account numbers.

Spyware - This ill-intentioned software installs itself onto computers and captures information without your knowledge, such as account numbers and passwords.

Shoulder Surfing - Criminals look over your shoulder and watch you do things like fill out forms or enter ATM pins.

Vishing - Just like Phishing, but performed over a phone.

Credit Card Skimming - When criminals capture your credit card number. This crime can happen anywhere, including restaurants and tampered ATMs. Your information is then sold on the black market and used to create new credit cards so others can withdraw cash and make purchases using your account.



WHO IS AT RISK FOR IDENTITY THEFT?



The simple answer? Anyone with a social security number. While most cases involve individuals between the ages of 35 and 65, criminals have increasingly targeted other highly susceptible groups.⁹ These include children, seniors and military personnel.

CHILDREN

According to the Federal Trade Commission (FTC), victims under 18 are the fastest growing segment for identity theft in America.¹⁰ Minors are often targeted because they have pristine credit records, making it easier for criminals to open new accounts in their name. And since parents rarely monitor their child's credit reports or financial activity, the crime often goes undetected for long periods, potentially exposing the child to hundreds of thousands of dollars in debt.

COLLEGE STUDENTS

The risk for this group is very high. One main reason? Many colleges use Social Security numbers as student IDs (which appear on almost everything), making students especially vulnerable. And because this segment moves often and may neglect to forward mail, sensitive documents like pre-approved credit card offers can fall into the wrong hands.

FACTS

The culprit is typically a parent or guardian or anyone with access to a child's information⁷

Nearly 500,000 children each year are victims of identity theft¹¹

Identity theft against minors can haunt them for decades

Identity thieves can obtain a minor's Social Security number and personal info from many sources, including medical records, school files and online social networks

SENIORS

Unfortunately, there are many ways criminals can prey on the trusting nature of seniors. Identity theft is no exception. The most popular cases involve stolen Social Security numbers, which criminals (some who are close to the victim) can access in several ways. Take Medicare, the primary form of health insurance amongst the elderly. Because Medicare uses Social Security numbers to identify each of its nearly 44 million beneficiaries, seniors are particularly exposed to fraud – seniors who've spent a lifetime building a nest egg for themselves and their families.¹² With this information, thieves can call Medicare and change the victim's address to their own, collecting future checks and even generating other benefits for themselves. According to the FTC, identity theft for this group has nearly tripled since 2000.¹³



MILITARY

This segment has emerged as a prime target for identity thieves. As a group, members of the military tend to respect and appreciate others who have served. This allows predators to falsely position themselves as comrades and take advantage of others who trust them. And because Social Security numbers appear on over eight million military identification cards (often attached to possessions in transit and medical files), military personnel are increasingly vulnerable to identity theft.¹⁶



FACTS

In 2005, 11% of Americans over 65 reported an identity theft crime¹⁴

Seniors are often targeted by someone they know¹⁵

In a few cases, identity theft crimes have been linked to nursing home staff

Since the 1960's the Department of Defense has used a SSN on everything from dog tags to chow line rosters¹⁷

Thieves took computers containing sensitive data for nearly 26,000 active and retired military personnel¹⁷

Due to the number of people with access to military records and files, this group is particularly exposed to identity theft¹⁷

Thieves target lump sum payments made for deployment and bonuses

MEDICAL IDENTITY THEFT

Beyond the obvious financial damages, medical identity theft can also have life-threatening consequences. When an imposter obtains medical care under your name, your medical history changes, potentially leading to a future misdiagnosis or denied coverage. So while fraudulent medical bills can cause years of stress, the wrong medication or hospital treatment could prove fatal. And because the Health Insurance Portability and Accountability Act (HIPAA) makes it very difficult to “fix” the consequences of medical identity theft, prevention of this crime truly is the best medicine. This year alone, it’s estimated that over 500,000 Americans will be unknowingly victimized by medical identity theft.¹⁸



DON'T LOSE YOUR CAP.

Some medical identity thieves steal more than hospital care. They can actually take dollars away from your lifetime cap. Let's say you have a \$1 million cap with your healthcare provider. If a criminal receives \$70,000 of care under your name, then you've just lost a huge chunk of your available medical coverage.



MORTGAGE IDENTITY THEFT

Just how serious is mortgage identity theft? In 2004, the FTC reported that \$429 million was stolen in fraud involving home loans.¹⁹ This type of crime typically happens when an identity is stolen and used on a loan application for a new home purchase or line of credit. All a thief needs is a few personal details, like your Social Security number, date of birth and some credit information. Even more surprising, identity thieves can sell your property without you knowing. This scam usually involves one criminal who steals your identity and sells the property to an accomplice. After they abscond with the mortgage money, victims are left behind to repair the damage.

INTERNET IDENTITY THEFT

The Internet is a virtual playground for identity thieves. With hundreds of millions of people openly exchanging information, criminals have devised many ways to intercept and steal personal data online. One popular method is called phishing, where someone impersonates a company or important authority and emails you an official looking request for things like your address, bank account number or passwords. Criminals also like to target social networking sites, where people freely post photos and volunteer intimate details. With minimal effort, "social engineers" can gather pictures, infiltrate friends lists, and assemble enough personal information to forge an identity.



FACTS

In the past year, fraudulent companies phishing for information grew by 50%²⁰

Since 2003, 1 in 8 Americans has been affected by Internet identity theft²¹

Over \$3 billion is lost to phishing scams every year²⁰



Amy had her identity stolen. Twice.

The first time, Amy received a letter from a collection agency regarding a cell phone account that was \$2,000 past due. Discovering her identity had been stolen, she called her provider and was forwarded to their fraud department. After countless dead-end conversations, the FBI informed Amy that her information had been sold by someone at a major credit bureau. After finally fixing the problem, an even worse crime hit. This time Amy received a collection letter for \$4,000 regarding another fraudulent cell phone account. The agency insisted she pay a portion immediately. They became nasty with her about paying the bill. When she called the phone company, they didn't believe her either. Worse yet, Amy says "The phone company wouldn't even give me the bill so I could call the numbers listed or see if I recognized any of them." After eventually filing a police report, the detective told Amy to place fraud alerts with the major credit bureaus. "I'm freaked out about giving out any information now," she said. "This can happen to anybody."

Brandon can't fix his damaged credit.

Brandon discovered his identity had been stolen when applying for his first home loan. There was \$23,000 of past due child support and more than \$5,000 of unpaid emergency room charges listed in his report. Since he didn't have any children and the hospital charges were from a number of different states, it was obvious that they were from someone using his identity. Brandon doesn't know how his identity was stolen, but believes the person only has his social security number and has been using a fake name. He filed a police report and got a case number, but they haven't been able to help. Brandon even went to the Attorney General of the state, but they weren't able to help with his case because the names and social security numbers didn't match on his documents, an obvious problem for a stolen identity. In his words, "If you're a victim, you have less rights than the criminal."

For more victim stories, visit the [Resource Center](http://www.trustedid.com) at www.trustedid.com

WHAT TO DO YOU IF YOUR IDENTITY IS STOLEN

Should you become a victim of identity theft or discover suspicious account activity, there are several immediate measures you can take to help minimize further damage and reclaim your identity.

1. FILE A POLICE REPORT WITH LOCAL LAW ENFORCEMENT.

A copy of this report can help you deal with creditors and collection agencies who demand payment for the fraudulent charges. If the police are hesitant to assist, you can request a "Miscellaneous Incident" report instead.

2. PLACE FRAUD ALERTS ON YOUR CREDIT REPORTS.

By calling any of the three major credit bureaus, you can place alerts that require creditors to verify your identity before issuing new credit.

As a TrustedID customer, we give you the option to place fraud alerts if your identity is at risk, and we will help you ensure your fraud alerts are renewed with the credit bureaus every 90 days.

3. CLOSE ACCOUNTS THAT MAY HAVE BEEN COMPROMISED.

If you believe someone may have gained access to your personal accounts, it's important to call those companies and speak with their fraud or customer service department. Make sure to follow-up in writing and request any forms you may need to dispute claims. It's also wise to change your future passwords and PINs to prevent further tampering.



PROTECT YOURSELF MOVING FORWARD. USE TrustedID.

While things like credit monitoring services help, you're only alerted after the damage is done. That's why TrustedID offers over 15 points of proactive protection, including public and private database scanning for misuse of your personal information, and protecting your medical benefits and Social Security number. These additional measures ensure you have the comprehensive protection needed to stop identity theft before it happens. This way you can focus on living your life, not trying to reclaim it.



TrustedID. THE PROACTIVE SOLUTION

Simply put, TrustedID provides the comprehensive protection your identity needs to be properly safeguarded. Over 15 points that help shield you from identity theft. Better yet, TrustedID takes preventative measures, like scanning black market Internet areas to see if your information has been compromised and proactively protecting your Social Security number and bank accounts. Furthermore, TrustedID has professional On-Call Protection Specialists who are there for you.

DAILY PROTECTION TIPS

Identity theft begins with stolen information. Here are a few things you can do to reduce this risk and help protect your identity.

- Shred personal information before throwing away**
- Change online passwords frequently**
- Protect your Social Security number at all times**
- Don't respond to online requests for personal info**
- Use current anti-spyware and anti-virus software**
- Check your credit report often for irregularities**
- Make sure mail arrives to a secure or lockable mailbox**
- Keep personal information guarded at ATMs or banks**
- Before selling a computer, remove all personal files**
- Limit the amount of personal information on checks**

TrustedID PROTECTS YOU WITH OVER 15 POINTS OF PROVEN PROTECTION:

Expert On-Call Protection Specialists

\$1,000,000 service warranty²²

Coverage for your entire family

Anti-spyware and anti-virus protection

Medical benefits protection

Junk mail reduction

Scanning of black market Internet areas for your personal info

Credit card number scanning

Name and address scanning

Bank account number scanning

Social Security number scanning

Fraud alert reminders

Lost wallet protection

Free annual credit reports

Credit freeze



www.trustedid.com

STOP IDENTITY THEFT BEFORE IT HAPPENS.



PROTECT YOURSELF NOW WITH TrustedID.

Go to www.trustedid.com
or call 1-800-661-8181





SOURCES

1. Gartner study, 2007.
2. FTC, 2006. <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
3. Gartner study, 2007
4. Gartner study, 2007. <http://www.gartner.com/it/page.jsp?id=565125>
5. ITRC, 2004.
6. Gartner study, 2007.
7. Identity Theft: The Aftermath. Idtheftcenter.org, 2007. http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2007_20080529v2_1.pdf
8. FTC, 2006. <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
9. FTC, 2006. <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
10. FTC. <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
11. Main culprits in kids' ID theft? Family members, NBC News, 2005. <http://www.msnbc.msn.com/id/7045490>
12. The Basics, National Health Policy Forum, 2007. http://www.nhpf.org/pdfs_basics/Basics_Medicare.pdf
13. FTC. <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
14. Consumer Credit Counseling Service. <http://www.identitytheftcounseling.org/Statistics.htm#Age>
15. Senior Citizens Information and News. <http://seniorjournal.com/NEWS/Alerts/5-08-03IDTheftPoll.htm>
16. Privacy Rights Clearinghouse. Federal Agency Use: <http://www.privacyrights.org/fs/fs10-ssn.htm>
17. Military Personnel Prime Targets for ID Theft. USA TODAY, 2007. http://www.usatoday.com/tech/news/computersecurity/infotheft/2007-06-14-military-id-thefts_n.htm
18. Medical Identity Theft: The Information Crime that Can Kill You. World Privacy Forum, 2006. http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf
19. FTC. <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
20. Phishing Attacks Escalated in 2007; More than \$3 Billion Lost to These Attacks. Gartner, 2007. <http://www.gartner.com/it/page.jsp?id=565125>
21. Internet Identity Theft. Winferno Software, 2006. <http://articles.winferno.com/computer-fraud/internet-identity-theft/>
22. Terms and conditions may apply