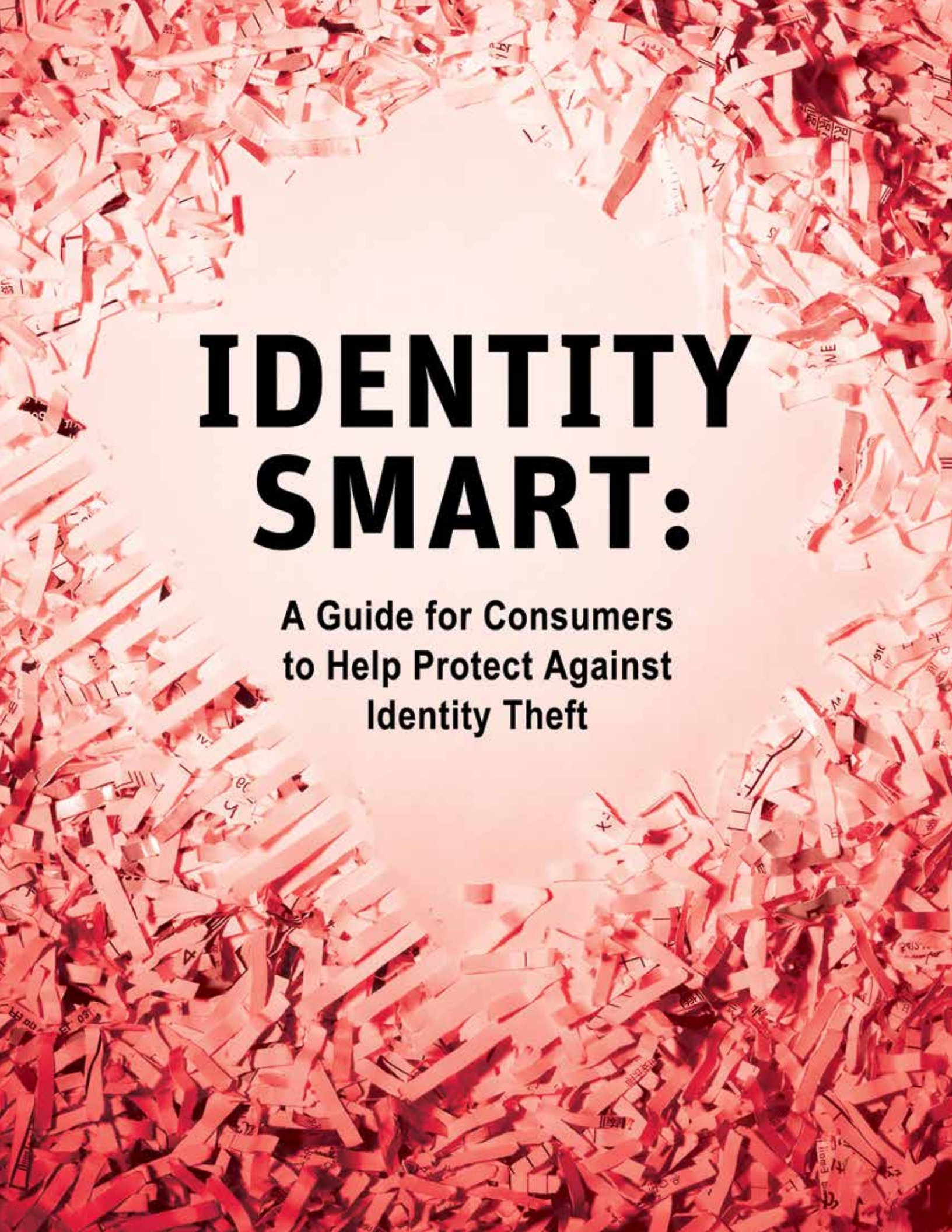


IDENTITY SMART:

A Guide for Consumers to Help Protect Against Identity Theft

IDENTITY ALERT:

The Fight to Defend Your Identity and Personal Information

A frightening crime with an untraceable weapon, identity theft is creating anxiety across the country. In fact, 1 incident every 3 seconds of identity fraud is occurring in households throughout America[1]. This horrible and personal crime can cause Americans to live their lives in fear—opening each monthly bank statement with bated breath.

With the anonymity of computer keyboards and high level technologies, imposters, and hackers can commit identity–related crimes on any unsuspecting victim, from anywhere in the world. With the nine simple digits of a Social Security number, or an electronic scan of your debit card, an identity thief can wreak havoc on your personal, legal or financial life for months or years—and sometimes with no detection at all.

It falls to you to raise your level of identity theft awareness—and to help defend yourself against a crime that can drain your time, your resources, and your good name.

[1] www.identitytheftassistance.org "Research and Statistics" Identity Theft Assistance Center, 2012.

WHAT IS IDENTITY THEFT?

According to the U.S. Department of Justice[2]:

"Identity theft is a crime. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain."

In short, identity theft can be defined as the fraudulent use of personal information to commit crimes. These crimes can often end in tax fraud and credit fraud, but are also perpetrated for insurance, medical or legal purposes.

[2] www.Justice.gov "What Are Identity Theft and Identity Fraud?"

IDENTITY THEFT: THE NUMBERS

How the Facts and Figures Affect Your Day-To-Day Life

The prospect of a faceless online hacker stealing your personal identity information may not resonate with you at first—at least not until you get a frightening look at the numbers that tell the true story of identity theft.

Identity Theft was the number one complaint category for the past 13 years.[3]

The facts and figures compiled below shed some light on the growing problem:

- There were 12.6 million adult victims of identity theft in 2012[4]
- 1 in 20 consumers were victims of identity theft in 2012[4]
- The total loss in new account fraud, where a criminal uses a victim's personal information to open a new credit card or loan, reported just under $10 billion in 2012.[4]
- Credit card fraud accounts for two-thirds of all ID theft[5]
- 1 in 4 data breach letter recipients became a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging.[5]
- Government documents/benefits fraud (46%) was the most common form of reported identity theft, followed by credit card fraud (13%), phone or utilities fraud (10%), and bank fraud (6%). Other significant categories of identity theft reported by victims were employment-related fraud (5%) and loan fraud (2%).[3]
- Consumers reported paying over $1.4 billion in one million fraud-related cases. The median amount was $535. Of these fraud related cases 38% were contacted through email, 34% by telephone, and 9% through mail.[3]

[3] FTC. "Consumer Sentinel Network Data." January-December 2012.

[4] Sullivan, B. (2012). ID Theft on the rise again: 12.6 million victims in 2012, study shows. NBC News

[5] www.identitytheftassistance.org "Research and Statistics" Identity Theft Assistance Center, 2012

TO CATCH A THIEF

What You're Leaving Behind, and How Identity Thieves are Following the Trail

At work, on the town or sitting at home, you may be most vulnerable to identity theft when you least expect it. The following are some of the ways that identity thieves commit their crimes:

Phishing:

When fake emails are so well produced, they can be almost impossible to discern from legitimate ones. If you get tricked into clicking a link or submitting information through a fake email, you can find yourself on a long road to losing your passwords, your accounts and your data.

Online Shopping:

Consumers beware: shopping online has become a phenomenon around the world, and it's become one of the easiest ways to have your information stolen. Whether you're shopping at duplicate retail sites or through unsecured payment systems, your credit/debit cards could be at risk.

Data Breaches:

If you store personal information with any financial or business organization—even a huge insurance or medical corporation—your files could be compromised in a large-scale data breach.

Malware and Viruses:

With thousands of new viruses emerging daily, your computer and your information can be hacked through any website, Internet program or file sharing application.

Keystroke Logging:

On public computers, gas station pump displays and ATM keypads, criminals and hackers can install technologies to trace the buttons you press as you enter your card numbers, passwords and PINs.

P2P File-Sharing:

File sharing sites like Bearshare and Frostwire connect millions of users across the world — and they also connect unsuspecting music fans with viruses and open connections to unsecured networks.

Vishing:

Just as you can be tricked into divulging personal or protected information through a text message or website, you should also be wary of giving away information over the phone or through voice messages.

Shoulder Surfing:

Technology can make stealing identities easier than ever before, but old-fashioned ways are still just as effective at manipulating unsuspecting victims. Through shoulder surfing, any identity imposter can stand behind you with a camera—or even their own eyes—and watch as you enter passwords, personal identification numbers or private information.

Dumpster Diving:

Though not the most glamorous of identity stealing techniques, many criminals and fraud-minded imposters have taken to sorting through garbage to find old bills, recent receipts and other discarded personal information that can be easily stolen.

Change of Address:

This is a classic identity theft technique—thieves change the address where you receive mail and divert your personal information into the wrong hands.

Mail Theft:

Less creative than the change of address method, identity thieves will often simply search for unlocked or unwatched mailboxes, and rip the mail directly from the box itself—often in search of what can be found on credit card statements and tax forms or financial and personal information.

Stolen Wallet:

While some thieves might be after your wallet or purse for the money inside, many others will be more interested in the credit cards, Social Security card and other personal identification that you keep inside.

ATM Overlays:

Hidden from the untrained eye, thieves install these devices at ATM machines and gas pumps to steal your account information when you insert your card, and transmit it to a nearby computer.

THE OTHER SIDE OF IDENTITY THEFT

Out For More Than Just Money, Identity Thieves Can Take Advantage of Your Medical or Criminal History

When identity imposters decide to go after your PINs, passwords and personal information, they are not always simply trying to drain your bank accounts. They may be looking for something much more specific, and for something that can sacrifice your good name and your future plans.

Medical Identity Theft

You may not notice that your medical identity has been stolen until it comes time for you to receive medical treatment or make a claim on your health insurance. With this kind of theft, imposters will use your name or insurance information to get medical coverage that they may not be able to afford.

Criminal Record Identity Theft

One of the scariest forms of identity theft is when criminals go after your government records. Thieves could use your information to apply for a job, avoid paying a traffic ticket or dodge arrest.

Social Security Identity Theft

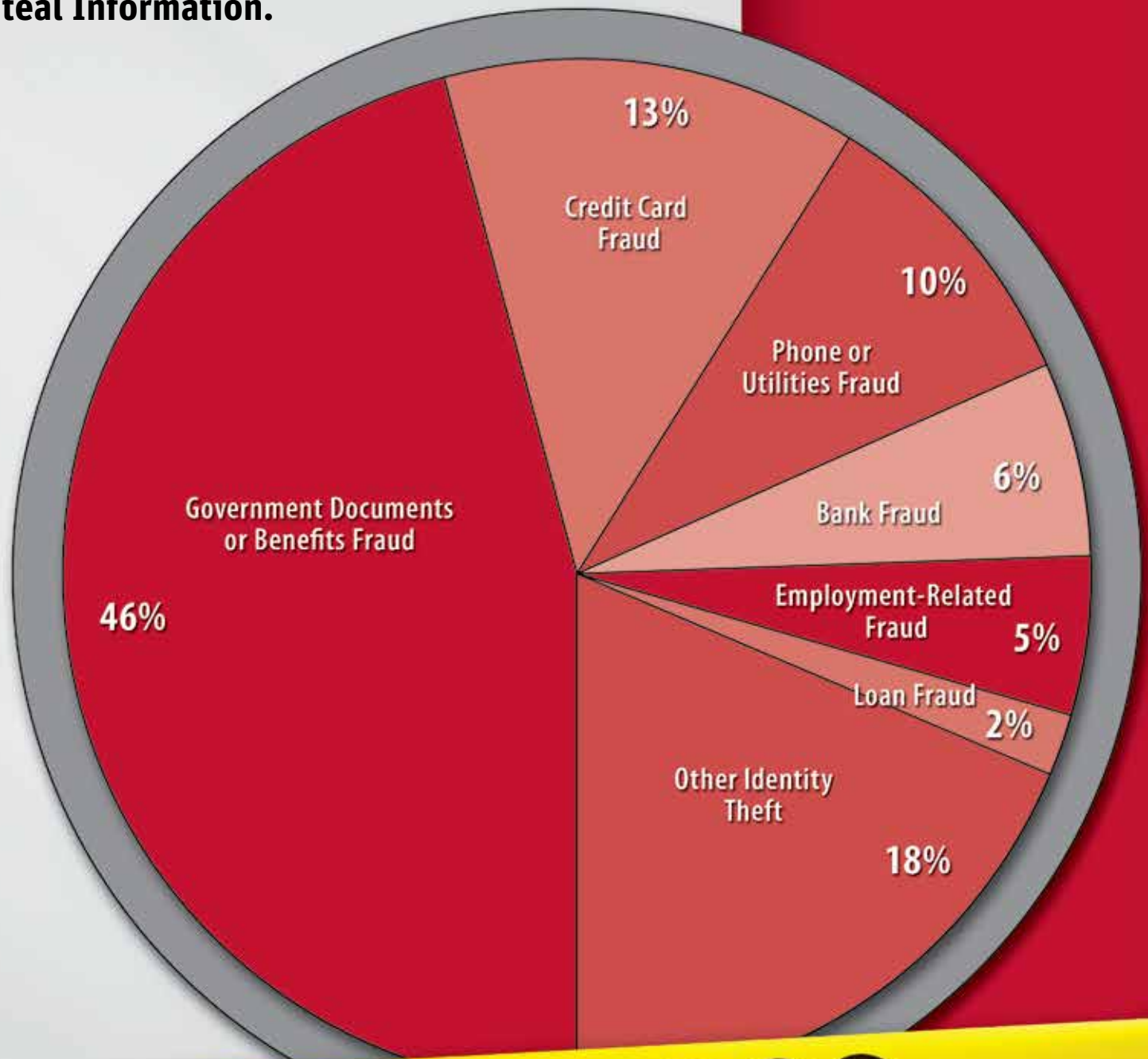
When your Social Security number is stolen by an identity thief, they can use the information to create new Social Security cards, access a number of public records or steal your name and personal information completely—assuming your identity.

Tax-Related Identity Theft

Using a stolen Social Security number, identity thieves can file fraudulent tax returns and receive refunds before you even file.

HOW IDENTITY THIEVES ARE STEALING YOUR IDENTITY

Based on FTC Complaints in 2012[3], These Are The Most Common Ways Thieves Steal Information.



DO NOT CROSS

[3] FTC. "Consumer Sentinel Network Data." January-December 2012

HELP STOP IDENTITY THEFT BEFORE IT HAPPENS

Follow These Precautions and Protection Tips To Set Up a Line of Defense Against Imposters

In the Mail

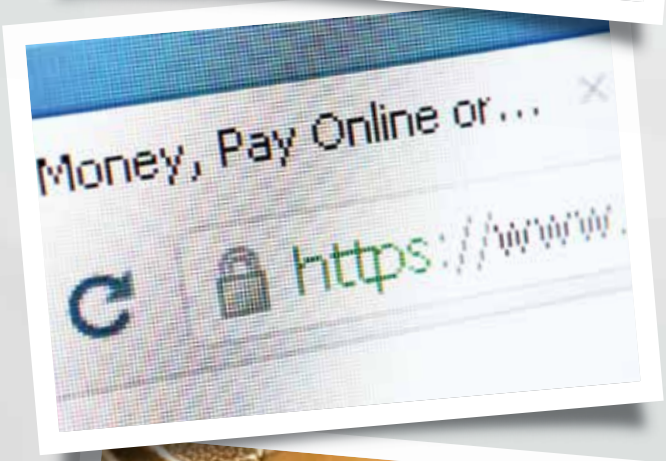
- Avoid placing outgoing mail into unlocked curbside mailboxes.
- Add a slot or a lock to your mailbox at home to prevent access to your private mail.
- Do not write account numbers or personal information on the outside of your envelopes.
- Have the post office hold your mail if you will be leaving town for more than a day or two.

Shopping Online

- Make sure you are doing business or shopping on a secure site before you provide any information. Make sure the site features a lock in the search bar and uses an “https” address.
- Check your billing statements for the company you purchased from to verify the correct amount and the correct purchase information.
- Avoid shopping from public Wi-Fi hotspots.
- Strengthen your shopping website passwords before making any purchases, and be sure to share only the necessary information when creating a login account or page.

Credit and Debit Cards

- When possible, use credit cards instead of debit cards. If your information is stolen from a debit card, an imposter can drain the cash from a checking or savings account—instead of running up your bill on a credit card.
- Make sure that cashiers swipe your credit or debit cards in front of you, and are not swiping them multiple times or through separate machines.
- Check your entire statement every time you receive it in the mail for your debit card or credit card, and be sure to account for every purchase or withdrawal. If banking online, check your statements as often as possible.
- Cancel your card immediately if you notice any suspicious charges or activity.
- Do not carry more debit or credit cards than are absolutely necessary.



At the Bank

- Use traveler's checks when possible, which are more difficult to duplicate than personal checks.
- Investigate if you are receiving late statements or late correspondences from your bank.
- Avoid giving personal information over the phone to anyone who claims they are working for a bank or credit card company (unless you previously initiated the contact).
- Use direct deposit when possible to avoid having a check that can be stolen from a payroll department or from the mail.

In Your Wallet/At Your Home

- Invest in a cross-cut shredder for all of your personal, financial or legal records, documents or correspondences. Throwing them away before shredding can leave them prone to dumpster diving imposters.
- Do not carry your Social Security card in your wallet or your purse. Keep it in a safe place at home, and only bring it out when you need it.
- Retrieve your mail promptly, and be sure to investigate if your mail is irregularly late or misses a day.
- Keep your wallet and purse secured when you are out in public, and avoid carrying more identifying personal information than is necessary.

The Last Line of Defense

- Use safe Internet passwords with a combination of letters and numbers. Do not make the passwords too obvious, use them for too many accounts, or keep them written in plain sight.
- Do not give your credit card information over the phone, unless you made first contact with the company.
- Be suspicious of any unexpected emails asking for personal information.
- Destroy the hard drive of your computer if you are selling it or discarding it. Beyond just erasing the hard drive, it should be physically destroyed.
- Safeguard your personal information at all costs, and educate yourself as much as possible about the many scams, imposters, hacks and schemes that are used to procure personal information.

HOW TO PICK UP THE PIECES AFTER IDENTITY THEFT

If You're the Victim of an Identity-Related Crime, Here's How You Can Begin to Repair the Damage

Step 1: Contact the Police

Instead of sitting stunned or helpless after an identity crime is discovered, you should take action right away. Start by contacting your local police or sheriff's department. Prepare and provide as much information as possible about what may have led to the identity theft.

Once your report is filed, you should be sure to do the following:

- Report the crime to your state law enforcement (to take advantage of recently toughened state laws regarding identity crimes)
- Obtain a copy of the police report to pursue your case with creditors
- Notify local authorities in the location where your identity was likely stolen

Step 2: Check Your Bank Statements and Balances

Your bank accounts should be the first place that you turn once a breach is detected.

Timing is important when it comes to protecting your savings, and taking the right steps can keep you from losing hundreds or thousands of dollars.

- Close your account right away and place stop payments on any stolen checks.
- Ask the bank to activate its check verification service to prevent identity imposters from cashing checks on your account
- Contact the Shared Check Authorization Network (800-262-7771) to find out if fraudulent checks are being passed in your name
- Order a free copy of the ChexSystems report that lists checking accounts opened in your name. ChexSystems, Inc.: 1-800-428-9623 or www.consumerdebit.com
- Contact businesses that accepted bad checks and report that you are a victim of identity theft.

If you think the fraud may exist beyond your current account—and an identity thief may have opened a new account in your name—contact your bank's consumer reporting service to close the account before it is too late.

Step 3: Contact the Credit Reporting Agencies

Because many identity thieves are looking to take advantage of open lines of credit, the three major credit reporting agencies should play a large role in helping you recover from your stolen identity.

Consumers can receive a free credit report yearly by visiting www.annualcreditreport.com. Monitoring your credit report will display all information about your credit, allow you to dispute any discrepancies, and give you notification if your credit is being used without your permission.

You should contact one of the reporting agencies as soon as possible to have your credit account flagged with a fraud alert. This agency is then required by law to contact the other two. To contact the three major agencies, use the following numbers:

Equifax:	**800-525-6285**	**www.equifax.com**
Experian:	**888-397-3742**	**www.experian.com**
TransUnion:	**800-680-7289**	**www.transunion.com**

Once you contact an agency:

-You can place an alert on your accounts for seven years after any identity theft
-You will receive two free credit reports within 12 months after your identity theft.
-A security freeze: a freeze can be placed on your credit by visiting any of the above credit reporting agencies.

If you suspect you are a victim of identity theft, each credit reporting agency has the option to place a free 90 day fraud alert on your account. Communication will be received from each credit reporting agency if any activity occurs on your credit.

Step 4: Connect with Your Creditors

Your creditors can be hit by identity theft as hard as you are, and it will be up to you to notify them as soon as possible of any suspicious activity on your account. The quicker you act, the easier the resolution will be.

You should contact your creditor's fraud department the second you discover any unauthorized charges, and you will be able to limit the charges that you are responsible for paying.

Step 5: Report the Details of Your Case to the Federal Trade Commission (FTC)

The national authority on identity theft and identity-related crimes, the FTC maintains an extensive database used to track, stop and catch identity thieves around the United States. You can contact the FTC through their toll-free hotline at 877-IDTHEFT www.ftc.gov.

STAY SECURE WHEN REPORTING YOUR IDENTITY THEFT

- Report the theft as soon as possible to ensure that you and your personal information are protected.
- Keep a copy or record of any and all correspondence with the authorities, your financial institutions and any credit reporting agencies.
- Avoid using originals of any personal documents when possible; use notarized and certified copies instead.
- Follow-up with all requests and actions, and be persistent in clearing your name and securing your information.

VICTIM ASSISTANCE

Contact the National Organization for Victim Assistance if you are a victim of identity theft for additional assistance at **www.trynova.org**

LifeLock

60 East Rio Salado Parkway
Suite 400
Tempe, AZ 85281

1-800-543-3562

LifeLock.com

For more information and resources, please visit: www.LifeLock.com/about/lifelock-in-the-community