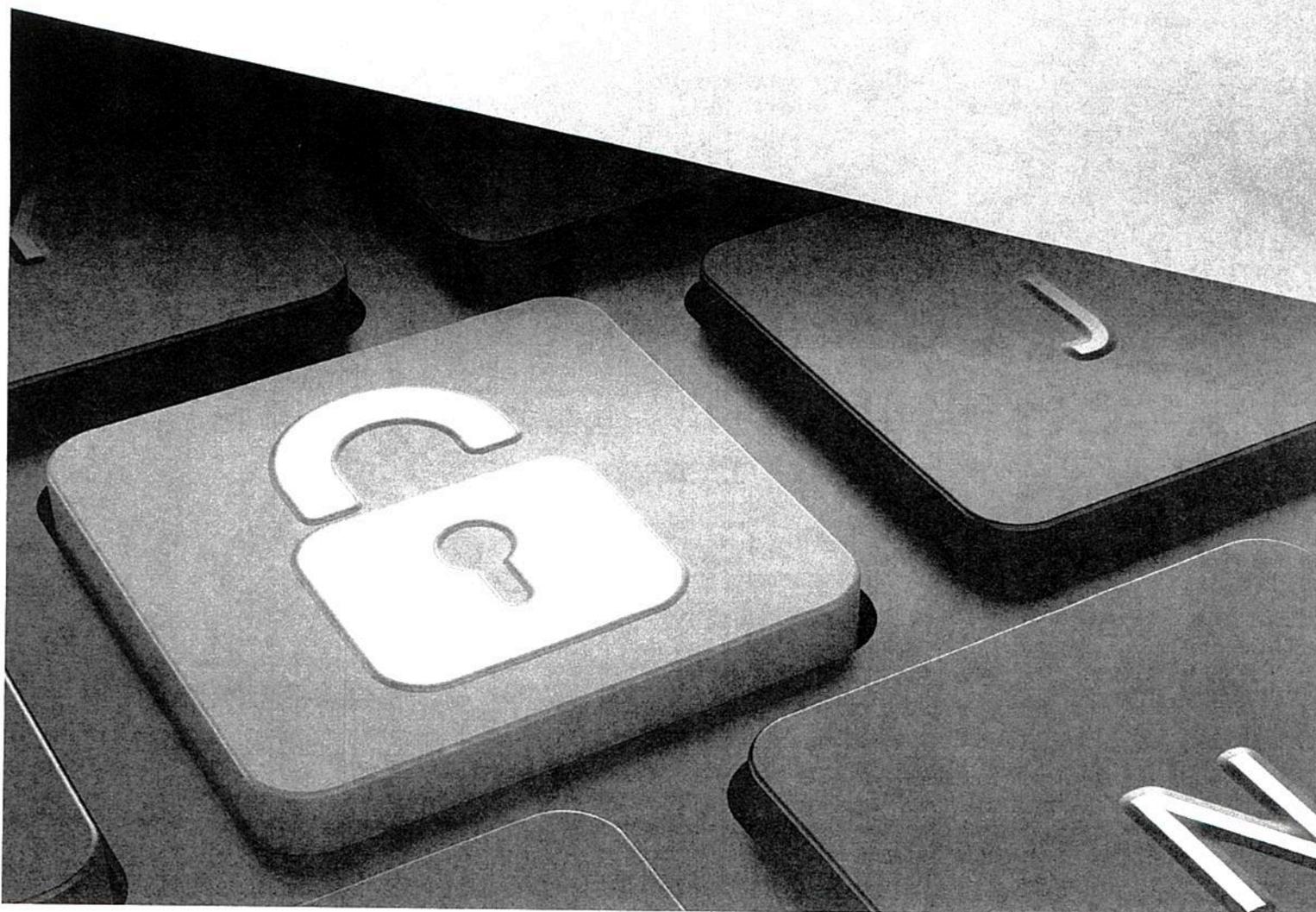

IDENTITY SMART

Resources to Help Against
Identity Theft and Fraud



IDENTITY ALERT:

The Fight to Help Defend Your Identity and Personal Information

A crime with an untraceable weapon, identity theft is creating anxiety across the country. In fact, every two seconds someone is a victim of identity theft¹.

With the anonymity of computer keyboards and high level technologies, imposters, and hackers can commit identity-related crimes on an 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.

¹Identity Theft Tracking Study, a commissioned survey conducted by Forrester Consulting on behalf of LifeLock, April/May 2014.



WHAT IS IDENTITY THEFT?

According to the U.S. Department of Justice:

"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."²

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

²"What are Identity Theft and Identity Fraud?" Welcome to the United States Department of Justice, June 2014. <http://www.justice.gov>

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 identifying information may not resonate with you at first—at least not until you get a shocking look at the numbers that tell the story of identity theft.

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

- Identity Theft tops list of consumer complaints for **14th** consecutive year.²
- **26** million US adults have been victim of identity theft in the past **12** months.¹
- **11%** of US adults have been a victim of identity theft in past **12** months.¹
- More than half (**50.5%**) of identity theft victims, in the past **12** months, were notified their personal information may have been a compromised due to a data breach.¹
- Total cost of identity theft in past **12** months was **\$19.5** billion.¹
- **41%** of identity theft complainants reported whether they contacted law enforcement. Of those victims, **74%** notified a police department. **61%** of those indicated a report was taken.³
- **1** in **3** individuals that were notified their personal information was part of a data breach, reported they experienced identity theft.¹
- Your medical information is worth **10** times more than your credit card number on the black market.⁴

¹ "Identity Theft Tracking Study," a commissioned survey conducted by Forrester Consulting on behalf of LifeLock. April/May 2014.

² Tressler, Colleen. "Identity theft tops list of consumer complaints for 14th consecutive year." Federal Trade Commission. February 27, 2014.

³ FTC. "Consumer Sentinel Network Data." January-December 2013.

⁴ Humor, Caroline, and Jim Finkle. "Your Medical Record Is worth More to Hackers than Your Credit Card." Reuters. N.p., September 24, 2014.

TO CATCH A THIEF

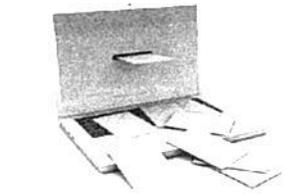
What You're Leaving Behind, and How Identity Thieves are Following the Trail

You may be more vulnerable to identity theft when you least expect it. The following are some of the ways that identity thieves commit their crimes:

Old School Methods:

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.



Dumpster Diving:

Though not the most glamorous of identity theft 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.



Mail Theft:

Identity thieves will often search for unlocked or unwatched mailboxes, and take the mail directly from the box itself—often in search of financial and personal information found on credit card statements and tax forms.



Shoulder Surfing:

Technology can make stealing identities easier than 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.



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.



Targeted Methods:

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.



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.



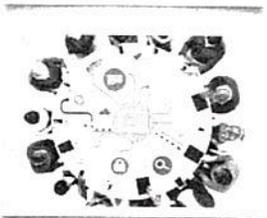
Online Shopping:

Whether you're shopping at duplicate retail sites or through unsecured payment systems, your credit/debit cards could be at risk.



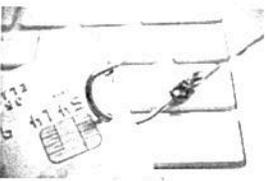
P2P File-Sharing:

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



Phishing:

When fake emails are so well produced, they can be very difficult 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.



Skimming:

A thief may place a skimmer within an ATM or any point of sale device in the attempt to capture all the information and data contained on the magnetic stripe of a credit, debit or ATM card.



Smishing:

This method takes place similar to phishing; but done through a Short Message Service (SMS) or text message. The message will direct you to visit a website or call a phone number. This is a scam to provide your personal information.



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.



THE OTHER SIDE OF IDENTITY THEFT

Thieves are out for more than just money, identity thieves can take advantage of your medical or criminal history.

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.

Government Documents or Benefits Fraud

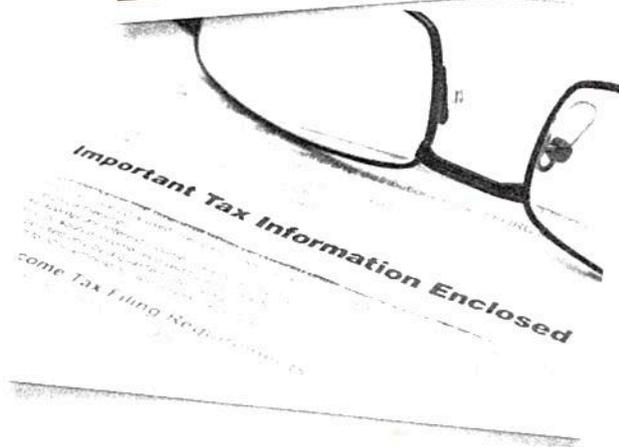
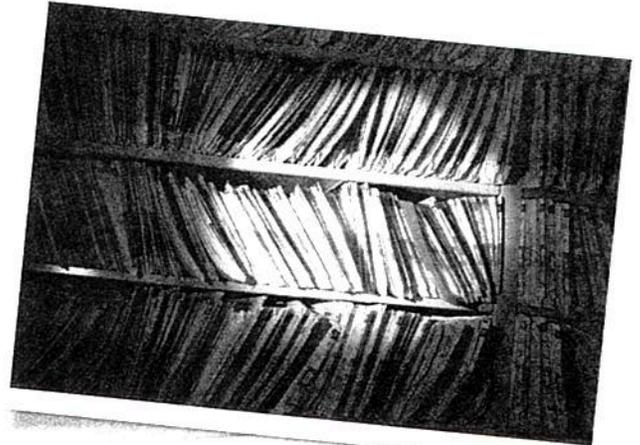
One scary form of identity theft is when criminals go after your government records. Thieves could use your information to apply for a job, avoid paying a traffic ticket or dodge arrest.

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.

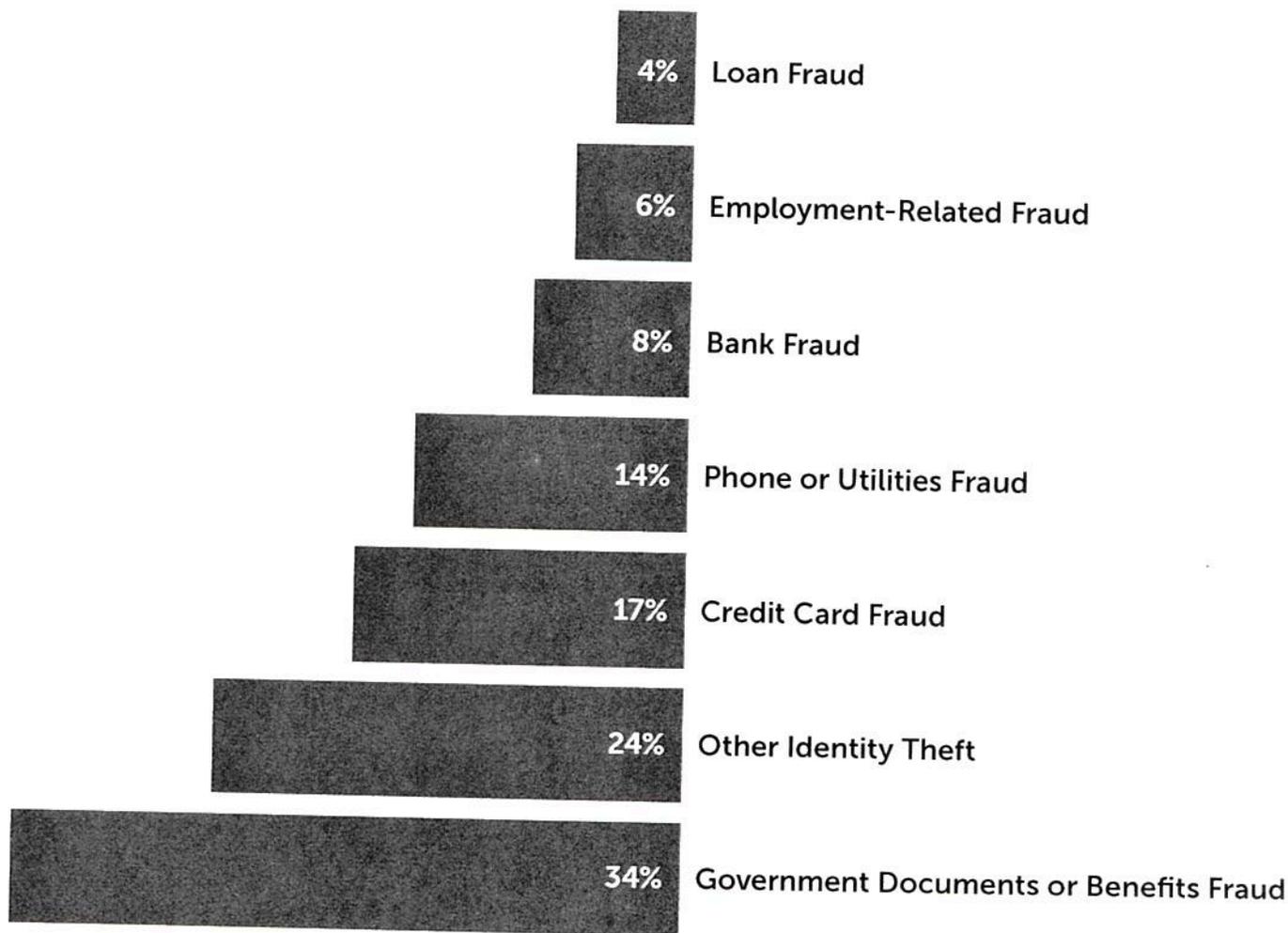
Tax-Related Identity Theft

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



How Victims' Information is Misused¹

These Are The Most Common Ways Thieves Steal Information*



* Note that 16% of identity theft complaints include more than one type of identity theft in Calendar Year 2013

TOP TEN STATES FOR IDENTITY THEFT COMPLAINTS¹

- | | | | | |
|------------|---------------|-------------|------------|--------------|
| 1. Florida | 3. California | 4. Nevada | 7. Arizona | 9. New York |
| 2. Georgia | 4. Michigan | 6. Maryland | 8. Texas | 10. Illinois |

STEPS TO HELP REDUCE VULNERABILITY

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 lock to your mailbox at home to minimize 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 an extended time period.

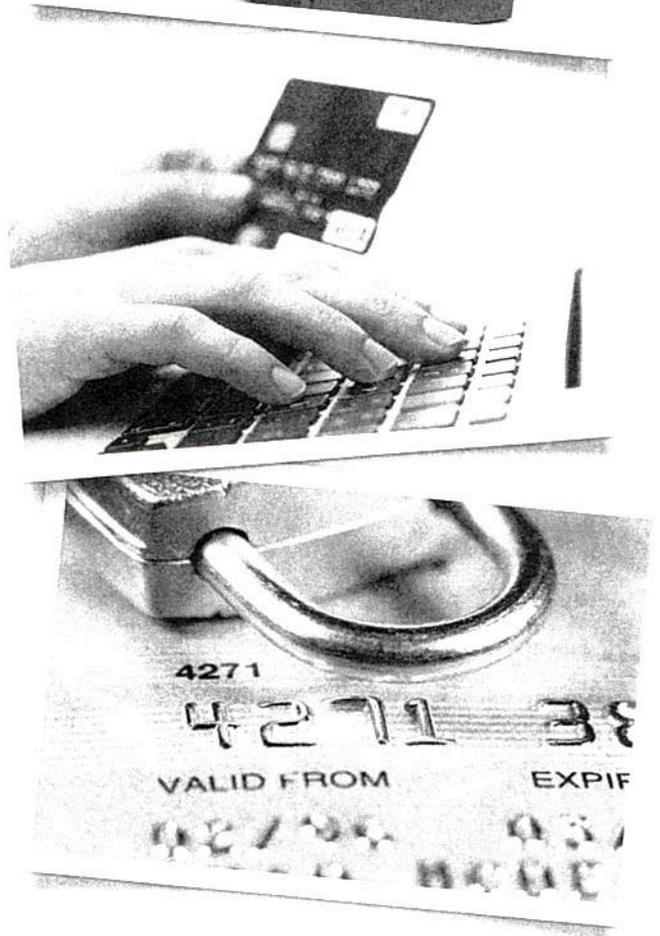
Shopping Online

- Ensure you are on a secure site before entering your personal information. Make sure the sites features a lock in the search bar and uses an "https" address before entering your personal information.
- 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.
- When creating a login account or page, and only share necessary information. Use symbols, numbers, and letters to create a strong password. Example: M**nSh\$ne357.



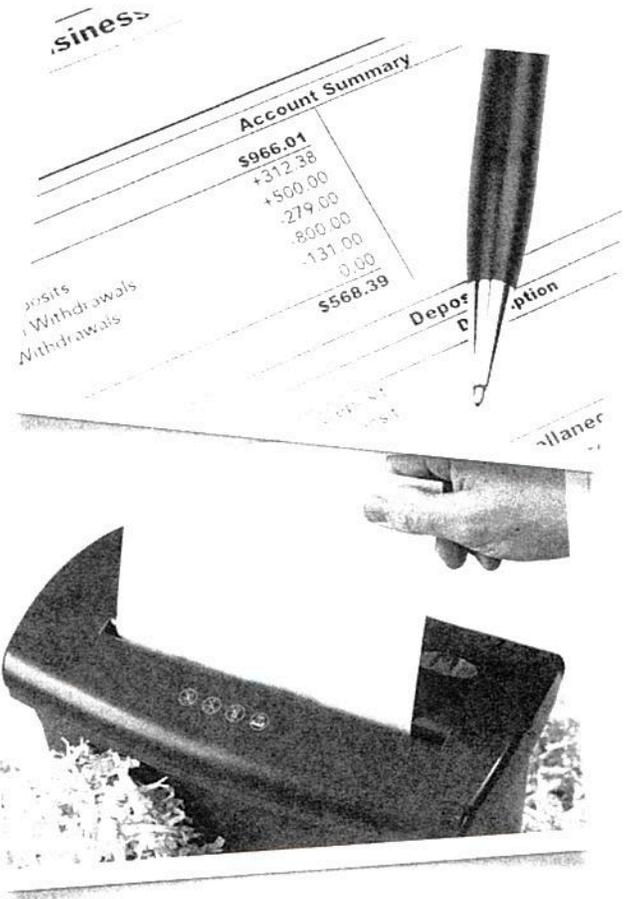
Credit and Debit Cards

- 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 or online 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 or utilize a mobile application for your bank to check your account. Set up thresholds and notifications for all accounts.
- 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

- 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 or recycling 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 personal identifying information.

The Last Line of Protection

- Use safe Internet passwords with a combination of letters (lower & upper case), numbers, and symbols. Do not make the passwords too obvious, use them for too many accounts or keep them written in plain sight. Set up a reminder to change your passwords every 3-4 months.
- 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.
- Help safeguard your personal information at all costs. Educate yourself as much as possible about the many scams, imposters, hacks and schemes that are used to procure personal information.

17

HOW TO PICK UP THE PIECES

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

Step 1: Contact the Police

After an identity crime is discovered, you should take action right away.

- File police report. Prepare and provide as much information as possible about what may have led to the identity theft.
- Obtain the incident report number to pursue your case with creditors. In some situations, you will need a copy of your police report.
- Visit your state Attorney's General website to obtain resources regarding remediation and victim assistance.

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
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 as soon as possible.



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.

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 agencies. To contact the three major agencies, use the following information:

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 extended alert on your account for seven years with a valid police report showing that you have been a victim of identity theft.
- You will receive two free credit reports within 12 months after your identity theft.
- A security freeze can be placed on your credit report by visiting any of the above credit reporting agencies; fees vary by state.

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 report.

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 may be.

You should contact your creditor's fraud department as soon as you discover any unauthorized charges, and you may 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)

Complaints from consumers help the FTC detect patterns of fraud and abuse. The FTC would like to know more about your complaint. Please visit the website at www.ftccomplaintassistant.gov or call their toll-free hotline at 877-IDTHEFT.

VICTIM ASSISTANCE

Contact the **National Organization for Victim Assistance (NOVA)** if you are a victim of identity theft for additional assistance at www.trynova.org or **800-TRY-NOVA**.



60 East Rio Salado Parkway Suite 400 Tempe, AZ 85281 | 1-800-543-3562 | LifeLock.com

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