WOMPLE LLC

IDENTITY THEFT
"DON'T BECOME A VICTIM"

THE INFORMATION PROTECTOR

A Complete Identity Theft Protection Resource Guide

MURRAY MONTGOMERY, JR., CPP
"America's Most Dynamic Identity Theft Protection Speaker!"

“This Page Is Intentionally Left Blank.”

WOMPLE, LLC PUBLISHING

THE INFORMATION PROTECTOR
A COMPLETE IDENTITY THEFT PROTECTION RESOURCE GUIDE
2026 EDITION

To order copies or to request permission to reprint, contact the publisher at
Womple, LLC Publishing
email: info@womplellc.com

ISBN 978-0-9818265-0-9

Printed in the United States of America.

Womple, LLC Publishing
Email: info@womplellc.com

Back to Table of Contents

DEDICATED TO:

All the people of the world whose identity is at risk

Mom and Dad
For whom I will always love and cherish

Back to Table of Contents

“This Page Is Intentionally Left Blank.”

Back to Table of Contents

Acknowledgments

I would like to extend my deepest appreciation to the dedicated team of family members, advisors, consultants, businesses, friends, and countless others who unconditionally contributed to and supported my efforts in the creation of this book.

Back to Table of Contents

About the Author

Murray Montgomery, Jr., CPP, is the Founder, President and CEO of Womple, LLC. He has a Bachelor of Science Degree and is board certified in **Security Management** by the American Society for Industrial Security (ASIS) International organization as a **Certified Protection Professional (CPP).**

Murray is a retired law enforcement and security professional with over twenty (20) years of experience protecting the citizens of the United States at the local, state and federal level.

Murray is an **Identity Theft Protection Expert**, delivering effective identity theft protection strategies in an informative and entertaining manner through keynote and break-out presentations, workshops, seminars, and other learning platforms.

Murray is also the author of **THE INFORMATION PROTECTOR:** ***A Complete Identity Theft Protection Resource Guide.*** The guide is packed full of helpful identity theft protection information, tools and strategies.

Murray believes passionately that by empowering consumers and businesses with effective identity theft protection information, tools, and strategies…then and only then will they be prepared to fight back against identity theft criminals and protect their credit, reputation and good name.

Back to Table of Contents

Link - Active Table of Contents

Back to Table of Contents

Back to Table of Contents

Introduction

IDENTITY THEFT…The Fastest Growing Crime in America!

THE INFORMATION PROTECTOR: A Complete Identity Theft Protection Resource Guide was written to provide consumers and businesses with a single resource to aid in minimizing their exposure to the crime of identity theft. The goal of this guide is EMPOWERMENT! Once you are empowered, you will feel confident that you have the information you need to fight back against this destructive crime

Below are some facts from the Federal Trade Commission (FTC) that will help you better understand the importance of protecting your identity:

- ✓ Almost 17 million Americans become victims of identity theft each year
- ✓ Identity thieves attack businesses and people of all ages
- ✓ Identity theft victims spend on average 120 hours and $3,000 to recover their credit and good name

By using this guide, you will learn how to:

- ✓ Protect your identity
- ✓ Avoid becoming a victim of identity theft
- ✓ Respond appropriately if your identity is stolen
- ✓ Report identity theft properly and avoid legal problems
- ✓ Restore your credit and good name

Back to Table of Contents

SECTION 1

Back to Table of Contents

DEFINITION OF IDENTITY THEFT

When someone obtains your personal identifying information (PII) such as your name, address, date of birth, social security number, etc., without your permission to commit fraud or some other type of crime.

WHAT IS YOUR IDENTITY

Listed below are several PII items that describe your identity:

- ✓ Full Name
- ✓ Social Security Number
- ✓ Bank Account Numbers
- ✓ Date of Birth
- ✓ Addresses
- ✓ Mother's Maiden Name
- ✓ Automated Teller Machine (ATM) Personal Identification Number (PIN)
- ✓ Credit Card Numbers
- ✓ Driver's License Number
- ✓ Telephone Numbers
- ✓ Email Addresses
- ✓ Usernames and Passwords
- ✓ Medical Information
- ✓ Birth Certificate
- ✓ Passport

Back to Table of Contents

WHAT TYPE OF INFORMATION DO IDENTITY THIEVES WANT MOST

Anything you can do to keep criminals away from your personal data helps to reduce your risk of identity theft. Following is a list of items identity thieves covet most:

- ✓ Your Name, Address, and Phone Number(s)
- ✓ Your Date of Birth
- ✓ Your Social Security Number
- ✓ Your Driver's License Number
- ✓ Your Credit and Debit Card Information
- ✓ Your Bank Account Information
- ✓ Your Mother's Maiden Name
- ✓ Your Username and Password
- ✓ Passport
- ✓ Birth Certificate

Back to Table of Contents

SECTION 2

Back to Table of Contents

HOW IDENTITY THIEVES GET YOUR IDENTITY INFORMATION

- ✓ Steal your wallet or purse (driver's license, credit/debit card, checkbook, etc.)
- ✓ Steal mail from your unsecure home or work mailboxes
- ✓ File a "Change of Address Request" with the postal service to re-route your mail
- ✓ "Red-Flagging" – flip-up your unsecure home mailbox red flag to notify the postal service person you have outgoing mail for pick-up
- ✓ Burglarize your home, business, or automobile and remove items with your personal identifying information (PII) on them
- ✓ "Dumpster Diving" – steal/rummage through your trash for PII
- ✓ "Pretexting" – fraudulent telemarketing calls and email messages to capture your PII
- ✓ "Skimming" – copy magnetic strip information from the back of your credit, debit, ATM, and other plastic cards
- ✓ "Shoulder Surfing" – use digital cameras and smart phones to capture your ATM and point-of-sale terminal personal identification number (PIN) information
- ✓ "Eavesdropping" – listen to your telephone and mobile phone conversations
- ✓ "Computer Hacking" – hackers gain access to your computer to steal your PII
- ✓ "Mobile Hacking" – identity thieves use malware and viruses to steal your PII from your mobile devices (smart phone, iPad, laptop, etc.)
- ✓ Install malware or virus software on your digital devices to steal your PII
- ✓ Data lost or stolen from businesses, governments, and educational institutions
- ✓ Collect credit, debit, and ATM card receipts
- ✓ "War-Driving" – remotely steal your PII from your unsecure wireless network
- ✓ "Evil Twinning" – create fraudulent websites on unsecure public wireless network and hotspots to steal your PII

Back to Table of Contents

HOW IDENTITY THIEVES USE YOUR IDENTITY INFORMATION

- ✓ Open new accounts in your name
- ✓ "High Jack" existing accounts in your name
- ✓ Obtain a driver's license in your name
- ✓ Obtain a passport in your name
- ✓ Create counterfeit checks in your name
- ✓ File for government benefits in your name
- ✓ File for bankruptcy in your name
- ✓ Make fraudulent withdrawals from your bank account
- ✓ Purchase cars and furniture in your name
- ✓ Set up utility services in your name
- ✓ Create counterfeit debit and ATM cards in your name
- ✓ Apply for credit cards in your name
- ✓ Apply for loans and mortgages in your name
- ✓ Apply for tax refunds in your name
- ✓ Commit crimes in your name

Back to Table of Contents

SECTION 3

Back to Table of Contents

HOW TO AVOID BECOMING A VICTIM OF IDENTITY THEFT

- ✓ Place a "security freeze" on your credit file maintained by the three major credit reporting agencies (Equifax, TransUnion, Experian)
- ✓ Place a 90-day "fraud alert" on your credit file with one of the three major credit reporting agencies (you only need to place it on one of the three and the others will be contacted to do the same). To keep the fraud alert on your credit file, it must be renewed every ninety (90) days
- ✓ Put your wallet/purse on an "Identity Diet" (i.e. remove as many unnecessary identity documents as possible from your wallet/purse and keep them in a secure location – safe deposit box or locked container/draw)
- ✓ Sign the back of all cards you receive from creditors (if not signed, creditors are not legally obligated to honor reimbursement agreements for cards lost/stolen)
- ✓ Photocopy all cards and identification documents (front and back) that you may carry in your wallet/purse and keep the copies in a secure location – safe deposit box or locked container/draw
- ✓ Safeguard your debit, credit, and ATM cards
- ✓ Purchase a "Cross-Cut or Micro-cut" paper shredder
- ✓ Shred all documents before disposing them in your trash
- ✓ Shred all old checks before disposing them in your trash
- ✓ Shred all unused pre-approved credit card and insurance offers that you receive in the mail before disposing them in your trash
- ✓ Shred all letter, envelope and magazine address labels
- ✓ Place a PIN or password on all accounts (bank, credit, debit, utilities, etc.), do not share them with others and keep them in a secure location
- ✓ Keep all usernames, PINs and passwords in a secure location and do not share them with others

Back to Table of Contents

- ✓ Request all new and replacement cards and checks be sent to a secure mailbox or your bank and not to your home address

- ✓ Request your free annual credit report from each of the three major credit reporting agencies (that's a total of three per year). A good strategy is to request one credit report every four months

- ✓ Regularly monitor your credit file from each of the three major credit reporting agencies to identify any fraudulent accounts or errors. Dispute them and have them removed as quickly as possible…if not, they will affect your credit score

- ✓ Cancel and close inactive accounts on your credit file

- ✓ Reconcile all bank statements against your check book register

- ✓ Limit the amount of personal identifying information (PII) you list on your checks (no SSN, driver's license number, telephone number, date of birth or address). REMEMBER, your checks flow through many hands before being processed for payment

- ✓ Use an "anti-fraud" check writing pen when writing checks to prevent "check-washing." They often can be found at most office supply stores

- ✓ Get a P.O. Box or install a "lock mailbox" at home

- ✓ Deliver all outgoing mail to the post office. NEVER leave outgoing mail in your unsecure mailbox at home (remember "red-flagging")

- ✓ Don't talk to strangers on the phone

- ✓ Don't open email messages from strangers

- ✓ Don't click on unknown links or pop-up advertisements while browsing the Internet

- ✓ Don't click on links sent to you in email messages

- ✓ Request all billing statements be sent to you electronically. GO PAPERLESS as much as possible (it minimizes the opportunity for identity thieves to steal your mail)

- ✓ Store all paper billing statements in a locked file cabinet or draw

Back to Table of Contents

- ✓ Pay bills online (as much as possible)
- ✓ Never use public computers, public hotspots or public wireless networks for personal use. Computers, public hotspots and wireless networks that are unsecure can potentially expose you to malware and viruses that identity thieves use to capture your usernames, passwords and other personal identifying information
- ✓ Secure your computer by installing anti-virus, anti-spyware/malware and firewall software and set them to update automatically
- ✓ Install and use secure browsers when surfing the internet and set them to update automatically
- ✓ Set your computer operating system to update automatically
- ✓ Opt out of receiving credit cards and convenient check offers
- ✓ Opt out of receiving telemarketing calls
- ✓ Opt out of receiving junk mail
- ✓ List your telephone numbers on the Do Not Call list
- ✓ Guard against "Shoulder Surfing"
- ✓ Guard against "Eavesdropping" of calls

Back to Table of Contents

HOW TO KNOW WHEN YOU HAVE BECOME A VICTIM OF IDENTITY THEFT

- ✓ Statements or other mail not arriving in your mailbox or email inbox on time or not at all
- ✓ Fraudulent accounts listed on your credit file
- ✓ Receive fraudulent statements from unknown creditors
- ✓ Merchants refusal to accept your checks for unknown reasons
- ✓ Debt collectors calling about fraudulent delinquent accounts in your name
- ✓ Denied credit, loans or job opportunities because of fraudulent delinquent accounts listed on your credit file
- ✓ Statements from medical providers for medical services you did not receive
- ✓ Medical claims rejected for services that had already been reimbursed in your name
- ✓ Fraudulent information listed on your "Explanation of Medical Benefits" statement
- ✓ IRS denies your claim for a tax refund because one had already been issued in your name
- ✓ Social Security Statement list income from an unknown employer
- ✓ Notified your privacy information was stolen because of a data breach incident
- ✓ Unauthorized withdrawals from your bank accounts
- ✓ Cancelled checks that don't match your check book register
- ✓ The police arrive at your door with an arrest warrant for a crime committed by someone else using your name

Back to Table of Contents

STEPS TO TAKE IF YOU BECOME A VICTIM OF IDENTITY THEFT

- ✓ Document who, what, when, where, and how you became a victim
- ✓ File a Police Report. Get a copy (preferred) or at a minimum, the number of the police report
- ✓ File a complaint with the FTC at https://www.identitytheft.gov Once you have completed the complaint, it will generate a FTC ID Theft Affidavit
- ✓ ORGANIZE! Establish an identity theft filing system to keep records of the incident
- ✓ Contact the three credit reporting agencies (Equifax, TransUnion and Experian) and place a "security freeze" on your credit file. You can lift, re-freeze or remove the security freeze on your credit file via the telephone or the internet using a PIN provided by each of the three credit reporting agencies. You should keep your PINs in a secure location
- ✓ Contact one of the three credit reporting agencies and place an "initial" 90-day fraud alert on your credit file (the company you call must tell the other two companies about your alert). The initial fraud alert also allows you to order 1 free copy of your credit report from each of the 3 credit reporting companies
- ✓ Review credit reports carefully for errors or fraudulent accounts. REMEMBER, it expires in 90 days; therefore, if you want the fraud alert to continue, you must renew it every 90 days…IT'S FREE
- ✓ Request a FREE copy of your credit file from each of the three credit reporting agencies
- ✓ Submit an identity theft "victim statement" to the three credit reporting agencies to be added to your credit file
- ✓ Contact creditors and banks immediately and notify them of fraudulent activities. Close any accounts that may have been compromised and establish new ones
- ✓ If possible, place or change PIN(s) and/or password(s) on all accounts
- ✓ Create an Identity Theft Report (FTC Affidavit + Police Report = Identity Theft Report)

Back to Table of Contents

- ✓ Once you have confirm you are a victim of identity theft and created an Identity Theft Report, contact each of the three credit reporting agencies and request an "extended" fraud alert be placed on your credit file. It will remain on your credit file for seven (7) years and provide some additional protections…IT'S FREE

- ✓ Send copies of original documents and all correspondence via certified mail return receipt requested. Keep original copies of documents in a secure location

- ✓ Keep a record of all monies spent and time lost recovering from being a victim

- ✓ Regularly monitor your credit file. Contact one of the three credit reporting agencies and set-up credit monitoring services. This is a PAID service

Back to Table of Contents

SECTION 4

Back to Table of Contents

HOW TO PROTECT ATM AND DEBIT CARDS

- ✓ Keep your PIN a secret. Don't use your address, birth date, phone or Social Security number as the PIN and try to memorize the number
- ✓ Be cautious about disclosing your account number over the phone unless you are dealing with a reputable company
- ✓ Draw a line through blank spaces on debit slips above the total so the amount cannot be changed
- ✓ Save your receipts to check against your monthly statements
- ✓ Shred old cards or cut through the account number before disposing them in the trash
- ✓ Open monthly statements promptly and compare them with your receipts. Contact the issuer immediately if you detect any discrepancies
- ✓ Keep a record (in a safe place separate from your cards) of your account numbers, expiration dates, and the telephone numbers of each card issuer so you can report fraudulent activity quickly
- ✓ Don't carry your PIN in your wallet or purse or write it on your ATM or debit card
- ✓ Carefully check ATM or debit card transactions before you enter the PIN or before you sign the receipt
- ✓ If you have access to your bank account online, check your ATM or debit card account activity frequently
- ✓ If your debit or ATM card is lost or stolen, contact the issuer immediately and follow up in writing. Request a new card with a different number, PIN and password. If possible, have the new card sent to your bank for pick up instead of having it mailed to your home
- ✓ Don’t use ATMs in non-banking locations. These ATMs may have a pen-size camera attached, phony keypads, or skimmers to capture your personal information and PIN

Back to Table of Contents

HOW TO PROTECT BANK ACCOUNTS

- ✓ Regularly monitor your bank account. If possible, try to use online banking as much as possible. It allows for regularly monitoring of your bank account between monthly statements
- ✓ Eliminate bank statements sent to you by mail. Request your bank statements be sent to you electronically. GO PAPERLESS
- ✓ Limit the amount of personal identifying information printed on checks. No driver's license, social security number, address or telephone number
- ✓ Guard your check book and keep it in a secure location
- ✓ Make a copy of a check and keep it in a secure location. You may need the information on the bottom (bank routing number and account number) to fight check fraud
- ✓ Use an "anti-fraud" check writing pen when writing checks to prevent "check-washing". They often can be found at most office supply stores
- ✓ If your check book is lost or stolen, contact your bank immediately. Close the account, open a new one and place a PIN/password on the new account. Also, request the bank contact the check verification service with which it does business to stop retailers from excepting your lost/stolen checks
- ✓ If your ATM or debit card is lost or stolen, report it immediately because the amount you can be held responsible for depends on how quickly you report the loss

Back to Table of Contents

HOW TO PROTECT MOBILE DEVICES

---

7 Steps to Secure Your Mobile Device

1. **Configure mobile devices securely**

   ✓ Enable auto-lock

   ✓ Enable password protection and create complex passwords (including letters, numbers and symbols)

   ✓ Avoid using auto-complete features that remember user names or passwords

   ✓ Ensure your Internet browser security settings are configured appropriately

   ✓ Enable remote wiping of all data stored on a mobile device

   ✓ Ensure that Secure Sockets Layer (SSL) protection is enabled, if available

2. **Connect to secure Wi-Fi networks and disable Wi-Fi when not in use**

   ✓ Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi

   ✓ Set Bluetooth-enabled devices to non-discoverable to render them invisible to unauthenticated devices

   ✓ Avoid joining unknown Wi-Fi networks

3. **Update mobile devices frequently. Select the automatic update option if available**

   ✓ Maintain up-to-date software, including operating systems and applications and have them update automatically

4. **Utilize anti-virus/anti-malware programs and configure automatic updates if possible**

   ✓ Install anti-virus/anti-malware software as it becomes available

Back to Table of Contents

5. **Use an encryption solution to keep portable data secure in transit**

   ✓ Data protection is essential. If confidential data must be accessed or stored using a mobile device, make sure you install an encryption solution

   ✓ Whenever possible, you should avoid using or storing confidential data on a mobile device

6. **Take appropriate physical security measures to prevent theft or enable recovery of mobile devices**

   ✓ For laptops, use cable locks

   ✓ Use tracing and tracking software

   ✓ Never leave your mobile device unattended

   ✓ Report lost or stolen devices immediately

   ✓ Remember to back up data on your mobile device on a regular basis

7. **Use appropriate sanitization and disposal procedures for mobile devices**

✓ Delete/wipe all information stored on a mobile device prior to discarding, exchanging, or donating it

Back to Table of Contents

HOW TO PROTECT YOUR CHECKS

- ✓ Never let merchants write your social security number on your checks. It's illegal in many states
- ✓ Limit the amount of information printed on your checks. Do not include your address, social security number, driver's license number, date of birth or phone number on your checks. Recommendation: only have your name printed on your checks. Merchants will ask for additional identity information if needed
- ✓ When ordering checks, if possible, request new checks be delivered to your bank for pick up instead of having them mailed to your home address
- ✓ Don't leave envelopes containing check payments for bills in an unsecure home or office mailbox (take them to the Post Office).
- ✓ Use an "anti-fraud" check writing pen when writing checks to prevent identity thieves from "washing" the ink from your checks, thus preventing the checks from being altered
- ✓ Shred all old checks and their carbon copies before disposing them
- ✓ Keep your checks and check book in a secure location
- ✓ Limit the use of checks as much as possible. Instead, use your bank's online-banking bill pay service
- ✓ In general, if an identity thief steals your checks, you need to stop payment, close the account, open a new one, place a PIN/password on the new account and ask your bank to notify ChexSystems, Inc. and the check verification service with which it does business

Back to Table of Contents

HOW TO PROTECT YOUR COMPUTER

- ✓ Install virus, spyware and malware protection software. Set them to update automatically
- ✓ Set your computer operating system to update automatically when security repairs and patches are recommended from your computer operating system's website
- ✓ Do not download files from strangers or click on hyperlinks from people you don't know. Opening a file could expose your system to a computer virus or a program that could hijack your computer or modem
- ✓ Do not respond to e-mails purporting to be from your bank, a government office, or other entities that requests your banking access credentials such as user IDs, passwords, PINs, etc. Always verify, first, before sharing such information
- ✓ Use a firewall, especially if you have a high-speed, or "always on," connection to the Internet, such as DSL or cable. The firewall allows you to limit uninvited access to your computer. Without a firewall, hackers may be able to take over your computer and access sensitive information
- ✓ Use a secure browser when accessing the internet. Secure browsers allow you to communicate with websites in a protected session by encrypting information that flows between you and the site. To verify your session is secure, look for https: instead of http: in the URL address line, and a secure symbol (for example, closed padlock or key)
- ✓ Limit financial information on your computer or other mobile devices. If you must store this information on these devices, use a "strong" password – that is, eight or more characters, including a combination of letters (upper and lower case), numbers, and symbols
- ✓ Avoid using an automatic login feature that saves your user name and password
- ✓ Always logout and close websites requiring your username and password
- ✓ Enable the "time out" feature that locks your computer when it is unattended

Back to Table of Contents

- ✓ Never leave your computer unattended while using any online banking or investing service

- ✓ Do not access your bank, brokerage, or other financial services information at Internet cafes, coffee shops, public libraries, airports and other public WI-FI locations. Malicious software may be installed on these wireless networks to trap your account numbers, usernames and passwords, leaving you vulnerable to being a victim of fraud

- ✓ Never share your password or PIN with anyone and never write down your password/PIN where others may find it. When selecting a password, don't use information easily linked to you (including your date of birth, pet's name, social security number, mother's maiden name, etc.). Change your password frequently for greater protection

- ✓ Delete any personal information stored on your computer before you dispose of it. Use a "wipe" utility program that overwrites the entire hard drive and makes the files virtually unrecoverable. Do not rely on the "delete" function to remove files containing sensitive information

- ✓ Setup your computer to request a unique "strong" password to gain access. Select a password that you do not use to access other accounts

- ✓ Setup your computer to go into password-required "sleep" mode after at a maximum of five minutes of inactivity

Back to Table of Contents

HOW TO PROTECT YOUR CREDIT CARDS

- ✓ Keep an eye on your credit card every time you use it, and make sure you get it back as quickly as possible. Try not to let your credit card out of your sight whenever possible
- ✓ Don't give out your account number over the phone unless you initiate the call. Never give your credit card info out when you receive a phone call. Legitimate companies don't call you to ask for a credit card number over the phone
- ✓ Never respond to emails requesting your credit card information and don't ever respond to emails that ask you to go to a website to verify personal or credit card information
- ✓ Never provide your credit card information on a website that is not a secure site
- ✓ Sign your credit cards as soon as you receive them
- ✓ Shred all pre-approved credit card applications you receive that you don't plan to use
- ✓ Don't write your PIN number on your credit card or have it anywhere near your credit card (in the event that your wallet or purse is lost or stolen). Try your best to memorize your PIN
- ✓ Never leave your credit cards or receipts lying around
- ✓ Shield your credit card number so that others around you can't copy it or capture it on a cell phone or camera
- ✓ Photocopy the front and back of all cards and keep the copies in a secure place. These copies should include all your cards account numbers, expiration dates, customer service numbers, and credit verification numbers. Update this list each time you receive a new credit card
- ✓ Only carry credit cards that you absolutely need. Don't carry extra credit cards that you rarely use
- ✓ Check your credit card statements promptly to detect any fraudulent charges. Save your receipts so you can compare them with your monthly statements

Back to Table of Contents

- ✓ If you find any charges that you don't have a receipt for -- or that you don't recognize -- report these charges promptly (and in writing) to the credit card issuer
- ✓ Shred anything with your credit card number written on it
- ✓ Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt where additional charges could be fraudulently added
- ✓ Never lend your credit card to anyone else
- ✓ If you move, notify your credit card issuers immediately of your new address

What To Do If Your Credit Cards Are Lost or Stolen

- ✓ If your credit cards are lost or stolen, contact the issuer(s) immediately
- ✓ Most credit card companies have toll-free numbers and 24-hour service to deal with these emergencies
- ✓ According to US law, once you have reported the loss or theft of your credit card, you have no more responsibility for unauthorized charges. Further, your maximum liability under federal US law is $50 per credit card -- and many credit card issuers will even waive that fee for good customers

Back to Table of Contents

HOW TO PROTECT YOUR MAIL

The U.S. Postal Inspection Service (USPIS) is the law enforcement arm of the U.S. Postal Service that investigates cases of identity theft. You can locate the nearest USPIS district office by visiting https://postalinspectors.uspis.gov/

Listed below are strategies to protect your mail:

- ✓ Use a secure locking mailbox or a P.O. Box to receive incoming mail
- ✓ Never place outgoing mail (at work or at home) in an open, unlocked mailbox. Take all outgoing mail to the post office. Also, during long absences, have mail held at the post office until you return
- ✓ Go PAPERLESS! Try and have as many of your bills and other statements sent to you electronically (via email)
- ✓ Make a list of all monthly bills and other statements and their expected delivery date. Investigate immediately if bills or statements do not arrive on time. An identity thief may have submitted a "Change-of-Address" request in your name to the postal service re-routing your incoming mail
- ✓ Never discard in the trash pre-approved credit and insurance offers and other mail with your personal identifying information listed on it. Always SHRED them first to prevent becoming a victim of identity theft by "dumpster-divers"
- ✓ Never flip-up the "red flag" on your unsecure mailbox at home to alert the postal employee you have outgoing mail for pickup. This also alerts identity thieves to the possibility that valuable outgoing mail is available for the taking
- ✓ Never leave mail lying around in your house for others to see. Place all unopened mail in a secure location until you are ready to open and process it
- ✓ Remove labels with your address from magazines, letters and "junk mail" and shred them before discarding them in the trash
- ✓ Opt-out of receiving pre-approved credit and insurance offer at www.optoutprescreen.com or call 1-888-5OPTOUT (1-888-567-8688)
- ✓ Limit the amount of unwanted "junk mail" you receive by removing your name and email address from member companies of the Direct Marketing Association (DMA) mail preference service at www.dmachoice.org

Back to Table of Contents

HOW TO PROTECT YOUR TRASH

Listed below are several identity items that should <u>NEVER</u> be thrown in the trash before they are shredded:

- ✓ Pre-approved credit card and insurance offers
- ✓ Credit/debit card receipts
- ✓ Convenience checks from credit card companies
- ✓ Pay stubs
- ✓ Copies of mortgage and loan documents
- ✓ Utility bills
- ✓ Social security annual statements
- ✓ Phone bills
- ✓ Credit card statements
- ✓ Cell phone bills
- ✓ Cancelled checks
- ✓ Insurance/medical statements
- ✓ Bank statements
- ✓ Car registration/insurance information
- ✓ Brokerage statements
- ✓ Expired driver's licenses
- ✓ Copies of tax records or notes
- ✓ Expired credit cards
- ✓ Magazine/envelope labels with your name and address

Back to Table of Contents

Additional information to protect your trash:

- ✓ Purchase a crosscut/microcut shredder instead of a horizontal shredder to shred your identity documents
- ✓ Don't discard sensitive documents at work unless you're sure they'll be shredded properly
- ✓ If possible, take your trash out just before it is due to be collected. Don't give identity thieves "dumpster-divers" time to go through your trash

Back to Table of Contents

SECTION 5

Back to Table of Contents

HOW TO REQUEST YOUR FREE ANNUAL CREDIT REPORT

The Fair Credit Reporting Act (FCRA) requires each of the nationwide consumer reporting companies — Equifax, Experian, and TransUnion — to provide you with a free copy of your credit report, at your request, once every 12 months. The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces the FCRA with respect to consumer reporting companies

A credit report includes information on where you live, how you pay your bills, and whether you've been sued or arrested, or have filed for bankruptcy. Nationwide consumer reporting companies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home

The three nationwide consumer reporting companies have set up a central website, a toll-free telephone number, and a mailing address through which you can order your free annual credit report

ONLINE:

- ✓ Request your free annual credit report online at www.annualcreditreport.com

BY PHONE:

- ✓ Call 1-877-322-8228; you will go through a simple verification process over the phone

Your reports will be mailed to you within 15 days. Please allow 2-3 weeks for delivery

BY MAIL:

- ✓ Complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The form can be found and printed from https://www.annualcreditreport.com/cra/requestformfinal.pdf

Your reports will be mailed to you within 15 days. Please allow 2-3 weeks for delivery

Regardless of how you request your report, you have the option to request all three reports at once or to order one report at a time. By requesting the reports separately, you can monitor your credit more frequently throughout the year

Back to Table of Contents

HOW TO REMOVE YOUR NAME FROM MAILING LISTS

✓ Direct Marketing Association (DMA) Mail Preference Service will allow you to receive less of the mail you do not want (junk mail). You may remove your name from individual organization lists. Complete the form and DMA will send it to their members and ask them to honor your preferences. Visit www.dmachoice.org to register your choices

HOW TO REMOVE YOUR NAME FROM PRE-SCREENED CREDIT & INSURANCE OFFERS

✓ If you would like to reduce the number of pre-screened credit and insurance offers that you receive, visit www.optoutprescreen.com or call 1-888-5OPTOUT (1-888-567-8688) to opt out of these offers. This is a free service to consumers offered by the major credit reporting agencies (Equifax, Experian and TransUnion)

HOW TO BE REMOVED FROM TELEPHONE CALL LISTS

Federal Trade Commission's National Do Not Call Registry

✓ Consumers who wish to decrease the amount of unsolicited telemarketing calls they receive should register with the Federal Trade Commission's National Do Not Call Registry at: https://www.donotcall.gov or by phone at 1-888-382-1222

✓ Telephone marketers and their service providers must honor the requests of consumers who have placed their telephone numbers on the registry

Back to Table of Contents

HOW TO BE REMOVED FROM EMAIL LISTS

The Email Preference Service (eMPS) is a consumer service sponsored by the Direct Marketing Association (DMA). Established in 1917, DMA is the oldest and largest national trade association serving the direct marketing field.

How can I be removed from email lists?

You may register with the eMPS removal file online at www.dmachoice.org.

How long is this registration good for?

Registration is good for five years after which you must renew your registration.

What happens after I request that my email address be removed?

When you register with eMPS, your name is placed on a "delete" file which is made available to companies.

Will registration with eMPS end all advertising mail?

No. You will continue to receive mail from companies with which you do business and from charitable or commercial organizations which do not choose to use eMPS. In addition, you may continue to receive email from many local merchants, professional and alumni associations, and political candidates. Unfortunately, there are many individuals who do not adhere to best business practices and do not remove people who do not wish to receive unsolicited email.

Back to Table of Contents

HOW TO REMOVE THE NAMES OF DECEASED INDIVIDUALS FROM MARKETING LISTS

The Deceased Do Not Contact List

The Direct Marketing Association (DMA) created in October 2005 a Deceased Do Not Contact List (DDNC) which all DMA members are required to honor. The DDNC list is available to companies and non-profit organizations for the sole purpose of removing names and addresses from their marketing lists.

What are the expected results?

When you register a name with DDNC, the person's name, address, phone number, and e-mail address are placed in a special do not contact file. All DMA members are required to eliminate these individuals from their prospecting campaigns.

The service is also available to non-members of DMA so that all marketers may take advantage of this service.

A new, updated file is distributed to members at least once every three months. Therefore the number of commercial contacts from DMA members should begin to decrease within three months.

How to Register

Go to Deceased Do Not Contact Registration and complete the online form. There is no charge to register for the DDNC list. Consumers will be asked for a credit card number to validate their identity and mailing address when registering. The credit card number will be used to authenticate and validate the consumer's identity through a no-charge transaction. As with many credit card verification programs, consumers may see an authorization pending for 3–7 days, and no charge will be issued to the monthly bill.

The DMA will not keep personal, identifiable information and will not use the information for marketing purposes.

Back to Table of Contents

SECTION 6

Back to Table of Contents

UNDERSTANDING THE IMPORTANCE OF AN IDENTITY THEFT REPORT

The Identity Theft Report is the **most** valuable tool you should have in your toolkit to use after discovering you have become a victim of identity theft. It has proven especially helpful when dealing with creditors, debt collectors, financial institutions and credit reporting agencies when attempting to regain your credit and good name.

What is an Identity Theft Report?

An Identity Theft Report is an official, valid, law enforcement report that documents a consumer's statement that they are a victim of identity theft. To discourage false filings, the Identity Theft Report exposes the consumer to criminal penalties if found to have filed false information. The Identity Theft Report should contain as much specific information as possible about the identity theft.

How do you obtain an Identity Theft Report?

An Identity Theft Report can be obtained by following these steps: (1) complete the FTC Identity Theft Universal Complaint and Affidavit form available at https://www.identitytheft.gov print a copy of the completed form (ID Theft Affidavit), and (3) take a copy of the completed ID Theft Affidavit to the police for inclusion in your police report. A police report that includes the victim's ID Theft Affidavit creates an Identity Theft Report.

Not all states require the police to take a report from an identity theft victim. If you are unable to obtain a report, you should provide the police with a copy of the Federal Trade Commission's memorandum to law enforcement on the importance of writing a police report for victims of identity theft, available at https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0088-ftc-memo-law-enforcement.pdf.

If you are still unsuccessful with your local police, attempt to make a report with another law enforcement agency such as the state police, sheriff, district attorney, or state attorney general. If you are unable to get any law enforcement agency to take your report, a section of the FTC ID Theft Affidavit allows you to indicate this fact.

How do you use the Identity Theft Report?

You can use your Identity Theft Report to invoke many of the rights granted to identity theft victims under the Fair Credit Reporting Act (FCRA). For example:

Back to Table of Contents

- ✓ **Blocking fraudulent information from a credit report:** You can stop a consumer reporting agency (CRA) from reporting information about you that is the result of identity theft by submitting your Identity Theft Report to the CRA. The CRA may ask for additional documentation to verify the validity of your request, such as your driver's license

- ✓ **Preventing a company from refurnishing fraudulent information to a CRA:** Once a company is informed by a CRA that you filed an Identity Theft Report and it has blocked the information it furnished, the company is prohibited from ever refurnishing that information to a CRA again

- ✓ **Preventing a company from selling or placing for collection debts that were created from identity theft:** Once a company is informed by a CRA that you filed an Identity Theft Report and it has blocked your account, the company is prohibited from selling, transferring, or placing for collection that debt

- ✓ **Placing an Extended Fraud alert:** An extended fraud alert requires potential creditors to contact you by phone or in person to verify the identity of a person applying for credit in your name. An extended fraud alert remains on your report for seven years

- ✓ **Getting documents from businesses:** You have the right to obtain documents related to fraudulent transactions resulting from identity theft. These records can be obtained by submitting your Identity Theft Report, along with proper proof of identification, to the company where the fraudulent transaction occurred

Back to Table of Contents

SECTION 7

Back to Table of Contents

HOW TO PLACE A SECURITY FREEZE ON YOUR EQUIFAX CREDIT FILE

Three ways to place, temporary lift or permanently remove an Equifax security freeze:

ONLINE

The easiest and fastest way is via Equifax's online process, which can be found at the following link:

https://www.freeze.equifax.com

BY PHONE

If you choose, you may place, temporary lift or permanently remove an Equifax security freeze by calling their automated line at 1-800-685-1111 (NY residents please call 1-800-349-9960).

BY MAIL

If you choose, you may place, temporary lift or permanently remove an Equifax security freeze by mail. Submit your request in writing to:

Equifax Security Freeze
P.O. Box 105788
Atlanta, Georgia 30348

When using the phone or mail options to place, temporary lift or permanently remove an Equifax security freeze, please be prepared to provide the following information:

- Your complete name including any suffix (e.g. Jr., Sr., etc.)
- Complete address
- Social Security Number
- Date of Birth

In addition, when using the mail option, please also send some proof of identification. Equifax will mail you a personal identification number (PIN) that will be required to temporarily lift or remove the security freeze. Payment, if applicable, to place, lift or remove an Equifax security freeze depends on your state of residents.

Back to Table of Contents

HOW TO PLACE A SECURITY FREEZE ON YOUR EXPERIAN CREDIT FILE

There are three (3) ways to place, temporary lift or permanently remove a security freeze on your Experian credit file:

ONLINE

The easiest and fastest way is via Experian's online process, which can be found at the following link:

www.experian.com/freeze

BY PHONE

If you choose, you may place, temporary lift or permanently remove an Experian security freeze by calling their automated line at 1-888-EXPERIAN or (1-888-397-3742).

BY MAIL

If you choose, you may place, temporary lift or permanently remove an Experian security freeze by mail. Submit your request in writing to:

Experian
P.O. Box 9554
Allen, TX, 75013

When using the phone or mail options to place, temporary lift or permanently remove an Experian security freeze, please be prepared to provide the following information:

- Your complete name including middle initial and any suffix (e.g. Jr., Sr., etc.)
- Complete address and previous addresses for the past two years
- Social Security Number
- Date of Birth

In addition, when using the mail option, please provide one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., **and** one copy of a utility bill, bank or insurance statement, etc. Experian will mail you a personal identification number (PIN) that will be required to temporarily lift or remove the security freeze. Payment, if applicable, to place, lift or remove an Experian Security Freeze depends on your state of residency.

Back to Table of Contents

HOW TO PLACE A SECURITY FREEZE ON YOUR TRANSUNION CREDIT FILE

There are three (3) ways to place, temporary lift or permanently remove a security freeze on your TransUnion credit file:

ONLINE

The easiest and fastest way is via TransUnion's online process, which can be found at the following link:

https://freeze.transunion.com

BY PHONE

If you choose, you may place, temporary lift or permanently remove a TransUnion security freeze by calling their automated line at 1-888-909-8872.

BY MAIL

If you choose, you may place, temporary lift or permanently remove a TransUnion security freeze by mail. Submit your request in writing to:

TransUnion
P.O. Box 6790
Fullerton, CA 92834

When using the phone or mail options to place, temporary lift or permanently remove a TransUnion security freeze, please be prepared to provide the following information:

- Your complete name including middle initial and any suffix (e.g. Jr., Sr., etc.)
- Complete address and previous addresses for the past two years
- Social Security Number
- Date of Birth

In addition, when using the mail option, please provide one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., **and** one copy of a utility bill, bank or insurance statement, etc. TransUnion will mail you a personal identification number (PIN) that will be required to temporarily lift or remove the security freeze. Payment, if applicable, to place, lift or remove a TransUnion Security Freeze depends on your state of residents

Back to Table of Contents

HOW TO PLACE A SECURITY FRAUD ALERT ON CREDIT FILES

There are three (3) types of security fraud alerts:

Initial or 90-day Fraud Alert – must be renewed after 90 days. Anyone can place an initial fraud alert on their credit file. You do not have to be a victim of identity theft.

Extended Fraud Alert – remains on credit file for seven years. A valid police report showing that you have been a victim of identity theft is required to place an extended fraud alert. Also, your name is removed from prescreened credit and insurance offers for five years.

Active-duty Military Fraud Alert – remains on your credit file for one year for active duty military personnel who are away from their duty station. Also, your name is removed from pre-screened credit and insurance offers for two years.

When you request an alert through one of the credit reporting agencies, your request is automatically sent to the other two agencies.

EQUIFAX

Phone: 1-800-525-6285

Online: https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Mail: Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348-5069

EXPERIAN

Phone: 1-888-EXPERIAN (888-397-3742)

Online: https://www.experian.com/fraud/center.html

Mail: Experian, P.O. Box 9554, Allen, TX, 75013

TRANSUNION

Phone: 1-800-680-7289

Online: https://fraud.transunion.com

Mail: TransUnion LLC, P.O. Box 6790, Fullerton, CA 92834

Back to Table of Contents

SECTION 8

Back to Table of Contents

IDENTITY THEFT VICTIM'S RIGHTS

An identity theft victim has the right to:

- ✓ File a report with law enforcement
- ✓ Place a Fraud Alert on your credit file
- ✓ Place a Security Freeze on your credit file
- ✓ Request one free copy of your credit report annually from each of the three credit reporting agencies
- ✓ Request credit reporting agencies block fraudulent information from appearing on your credit report
- ✓ Dispute fraudulent or inaccurate information on your credit report
- ✓ Close fraudulently opened or compromised accounts
- ✓ Request copies of all documents related to the theft of your identity
- ✓ Stop the collection of fraudulent debts by debt collectors
- ✓ Request that creditors block fraudulent information from being shared with credit reporting agencies

Back to Table of Contents

SECTION 9

Back to Table of Contents

APPENDIX: HELPFUL RESOURCES LIST

Resource Name	Resource Type	Telephone #	Website
Equifax	Credit Reporting Agency	(800) 525-6285	www.equifax.com
Experian	Credit Reporting Agency	(888) 397-3742	www.experian.com
TransUnion	Credit Reporting Agency	(800) 680-7289	www.transunion.com
Federal Trade Commission (FTC)	Federal Government Agency	(877) 438-4338	www.identitytheft.gov
US Postal Service (Fraud Dept)	Federal Government Agency	(800) 372-8347	https://postalinspectors.uspis.gov
Identity Theft Resource Center	ID Theft Protection Service	(858) 693-7935	www.idtheftcenter.org
Privacy Rights Clearinghouse	ID Theft Protection service	(619) 298-3396	www.privacyrights.org
Direct Marketing Association	Opt out of telemarketing offers and junk mail		www.dmachoice.org
Social Security Administration (Fraud Dept)	Federal Government Agency	(800) 772-1213	https://oig.ssa.gov
ChexSystems (Fraud Dept)	Check Verification Service	(800) 428-9623	www.chexsystems.com
TeleCheck	Check Verification Service	(800) 835-3243 or (800) 710-9898	www.telecheck.com

Back to Table of Contents

Free Annual Credit Report	Federal Government Service	(877) 322-8228	www.annualcreditreport.com
Social Security Earnings and Benefits Statement	Federal Government Agency	(800) 772-1213	www.socialsecurity.gov/mystatement
National Do Not Call Registry	Federal Government Agency	(888) 382-1222	https://www.donotcall.gov
Opt Out Pre-Screened Credit and Insurance Offers	Consumer Credit Reporting Agencies Service	(888) 5OptOut or (888) 567-8688	www.optoutprescreen.com
File an FTC ID Theft Complaint	Federal Government Agency	(877) 438-4338	https://www.identitytheft.gov
File an FTC Military ID Theft Complaint	Federal Government Agency	(877) 438-4338	https://www.identitytheft.gov
Deceased Do Not Contact Registration	Opt-Out Service for the Deceased		https://www.ims-dm.com/cgi/ddnc.php
FTC Memorandum to Law Enforcement	Federal Government Agency		http://www.consumer.ftc.gov/articles/pdf-0088-ftc-memo-law-enforcement.pdf
Equifax Security Freeze	Credit Reporting Agency	(800) 685-1111	https://www.freeze.equifax.com
Experian Security Freeze	Credit Reporting Agency	(888) 397-3742	www.experian.com/freeze
TransUnion Security Freeze	Credit Reporting Agency	(888) 909-8872	https://freeze.transunion.com
Equifax Fraud Alert	Credit Reporting Agency	(800) 525-6285	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Back to Table of Contents

Experian Fraud Alert	Credit Reporting Agency	(888) 397-3742	https://www.experian.com/fraud/center.html
TransUnion Fraud Alert	Credit Reporting Agency	(800) 680-7289	https://fraud.transunion.com
Free Application for Federal Student Aid (FAFSA)	Federal Government Agency for Student Aid		https://studentaid.gov

Back to Table of Contents

WOMPLE LLC

THEINFORMATION PROTECTOR: A Complete Identity Theft Protection Resource Guide is a must-read and an excellent resource packed with useful information to assist consumers and businesses in protecting their most valuable asset - "their identity".

A hands-on resource guide that empowers users with the strategies and tools needed to safeguard, protect and restore their identity, credit and reputation.

Topics Include:

- How to Avoid Becoming a Victim
- Steps to Take If You Become a Victim
- Identity Theft Protection Strategies and Solutions for:
  Businesses & Organizations, Consumers, Military Personnel, College Students, Seniors, the Deceased and much, much more!