WHAT IS IDENTITY THEFT?

Identity theft is when someone steals your personal information for their gain and your loss.

Personal information can include your Social Security number, birthdate, email address and passwords. Criminals could potentially empty retirement accounts, buy property and even commit crimes—all in your name. Sometimes it could take years before anyone notices and the restoration process can also be lengthy.

Please take the time to learn more in this handbook. When your level of identity theft awareness goes up, you can better defend yourself and educate others on how important it is to have identity theft protection.

IDENTITY THEFT BY THE NUMBERS

From data breaches to all you do online, it’s getting easier for criminals to steal your personal information.

1 in 4
The number of people in the U.S. who have experienced identity theft.¹

Every 2 seconds
someone’s identity is stolen.²
HOW CRIMINALS COMMIT ID THEFT

ID thieves are always looking for ways to steal your personal information. Here are some examples:

Mail Theft
By stealing your mail, thieves can get your personal information from bills, statements, etc.

Shoulder Surfing
Thieves stand behind you and watch as you enter passwords, personal identification numbers or private information.

Dumpster Diving
Thieves can go through your garbage to find old bills and recent receipts.

Keystroke Logging
On public computers, gas pump displays and ATM keypads, criminals can install technologies to record the buttons you press as you enter card numbers or passwords.

Data Breaches
Companies you do business with could be storing your personal information. If there’s a breach, your info could be compromised.

Vishing
Phone scams that request personal information either by a direct caller or through voice messages.

ATM Overlays
These are devices thieves install at ATM machines and gas pumps to steal your account information when your card is swiped.

Online Shopping
If you mistakenly shop at a fictitious retail website or through unsecured payment systems, your credit and debit cards could be at risk.

Change of Address
Thieves can change your address to steal your mail to commit identity theft.

The Dark Web
This is an underground, online community where criminals can go to buy and sell your personal information.

Malware & Viruses
Your computer can be hacked through websites, Internet programs or file-sharing networks allowing thieves to access your private personal information.

Phishing
These are fake emails that can look surprisingly legitimate. If you get tricked into clicking a link or providing information, thieves can get your passwords and account numbers.

Stolen Wallet
While some thieves might be after money, others are more interested in your personal identification to steal more than just cash.

Smishing
Phishing through a Short Message Service (SMS) or text message. The message will direct you to visit a website or call a phone number.
HOW THIEVES CAN USE YOUR STOLEN INFORMATION

Once a criminal has what they need, they can start doing bad things for their gain and your loss. Here are some examples:

**Tax-Related ID Theft**
By only using a stolen Social Security number and birthdate, identity thieves can file a fake tax return in your name.

**Drain Accounts**
Under your name, thieves can withdraw money or make major purchases like a house or car while you’re stuck with the bill.

**Medical ID Theft**
You may not notice this type of theft until it’s time for medical treatment or an insurance claim. Thieves can use your name or insurance information to receive medical care.

**Open New Accounts**
Thieves can open accounts for credit cards, loans, utilities and more in order to make purchases or steal funds. These accounts may not be detected for a year or more.

We don’t just alert† you to potential identity theft, we work to fix it.

Learn more at LifeLock.com/employer or contact your broker.

No one can prevent all identity theft.
† LifeLock does not monitor all transactions at all businesses.
LIFELOCK’S THREE-LAYERED APPROACH TO PROTECTION
Identity theft restoration. Don’t go through it alone.

**DETECT & ALERT**
We can detect a wide range of threats and will alert you by phone††, email or text if we find suspicious activity.†

**RESTORE**
If you become a victim of identity theft while a LifeLock member, a dedicated U.S.-based Identity Restoration Specialist will work with you from start to finish to help fix the issue.

**MILLION DOLLAR PROTECTION™ PACKAGE†††**
LifeLock helps protect you with reimbursement for stolen funds and compensation for personal expenses as a result of identity theft based on the limits of your plan and provides legal and expert assistance if needed with our Service Guarantee.†††

**THE LIFELOCK RESTORATION PROCESS**
If you become a victim of identity theft, our U.S.-based Identity Restoration Team will work to resolve the issues so you can focus on more important things. Here’s the eight-step process:

1. Member signs a Limited Power of Attorney form so LifeLock can work with merchants on the member’s behalf during the restoration process.
2. LifeLock will review credit, DMV and criminal background reports as well as financial statements and risk assessments.
3. LifeLock sets a seven-year fraud alert, and determines if lawyers, accountants or investigators are needed.
4. LifeLock will review the places where fraud occurred, submit applicable evidence, mediate claims and process credit disputes.
5. LifeLock submits insurance claims.
6. If needed, LifeLock will secure legal representation, represent member in court and pay court fees and costs.
7. LifeLock will document and organize correspondence in case of future ID fraud events.
8. Finally, LifeLock will request a release letter of fraud and check for a clean 90-day credit report.

Questions? Please visit LifeLock.com/employer or call 1-844-698-8640.

No one can prevent all identity theft.
† LifeLock does not monitor all transactions at all businesses.
†† Phone alerts made during normal local business hours.
††† Million Dollar Protection Package benefits are provided by a Master Policy issued by United Specialty Insurance Company, Inc. (State National Insurance Company, Inc. for NY State members). The Master Policy provides coverage for Stolen Funds Reimbursement and Personal Expense Compensation, each with limits of up to $25,000 for Standard members, up to $100,000 for Advantage members and up to $1 million for Ultimate Plus members. If needed, LifeLock will provide lawyers and experts under the Service Guarantee. Please see the policy terms, conditions and exclusions at: LifeLock.com/legal
WHY LIFELOCK?
Since there's a new victim of identity fraud every 2 seconds,¹ it only makes sense to go with the most recognized brand in the identity theft protection industry—LifeLock.²

• Founded in 2005
• Trusted by Over 4 Million Members
• Available From a Variety of Partners, Employers and Retailers
• Will Never Sell Your Data
• LifeLock was named a Top Trusted Website by the Online Trust Alliance in 2015 and 2016

“Don’t Wait Until Something Happens”

“Best decision I’ve made”

“Don’t Wait Until Something Happens”

“My purse was stolen with all identifying information from social security to address etc. I wish I had the coverage before the theft so I’d always have had peace of mind.”

Susan T, Member since Oct 2013

“Best decision I’ve made”

“I started using LifeLock right after I tried to file my taxes and was told that my SS# had already been submitted. My tax guy suggested I try LifeLock. Best decision I made! Now I have peace of mind.”

Jessie K, Member since Oct 2012
HERE ARE SEVEN PLACES WHERE A SMALL CHANGE CAN MAKE A BIG DIFFERENCE.

1. **Get LifeLock Identity Theft Protection**
   LifeLock sees a wide range of threats to help protect your identity
   24/7 Identity Protection Agents to answer any questions
   Million Dollar Protection™ Package†††
   Dedicated, U.S.-based Identity Restoration Specialist if you become a victim

2. **In Your Wallet/At Your Home**
   Use crosscut shredders for personal, financial or legal documents
   Retrieve mail promptly and investigate if your mail is late
   Don’t carry unnecessary identifying personal information
   Keep your wallet and purse secured when out in public

3. **Shopping Online**
   Create Internet passwords with combinations of letters and numbers
   Avoid creating passwords that are obvious or used often
   Keep passwords out of plain sight
   Make sure business and shopping are getting done on a secure site—you can tell if it’s secure by a lock featured in the search bar and uses “https” addresses
   Check billing statements for the correct company name, amount and purchase information
   Only share the necessary information when creating a login account

4. **Credit and Debit Cards**
   Use credit cards instead of debit cards when possible
   Take advantage of free credit monitoring services
   Don’t swipe your cards multiple times or through separate machines
   Make sure that cashiers swipe your cards in front of you
   Check your entire statement every month for every card and bank account
   Avoid carrying any debit or credit cards that aren’t absolutely necessary
   Cancel a card immediately if suspicious charges are found

5. **At the 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 contact
   Use direct deposit when possible
   Investigate late statements or correspondences from your bank
   Take advantage of free credit monitoring services

6. **Phone, Email and Computer**
   Be suspicious of any unexpected emails asking for personal information
   Physically destroy your hard drive before selling or discarding your computer
   Install reputable anti-virus software and keep it up-to-date

7. **In the Mail**
   Avoid placing outgoing mail into unlocked curb side mailboxes
   Don’t write account numbers or personal information on the outside of envelopes
   Have the post office hold your mail if you’re leaving town for more than a day or two