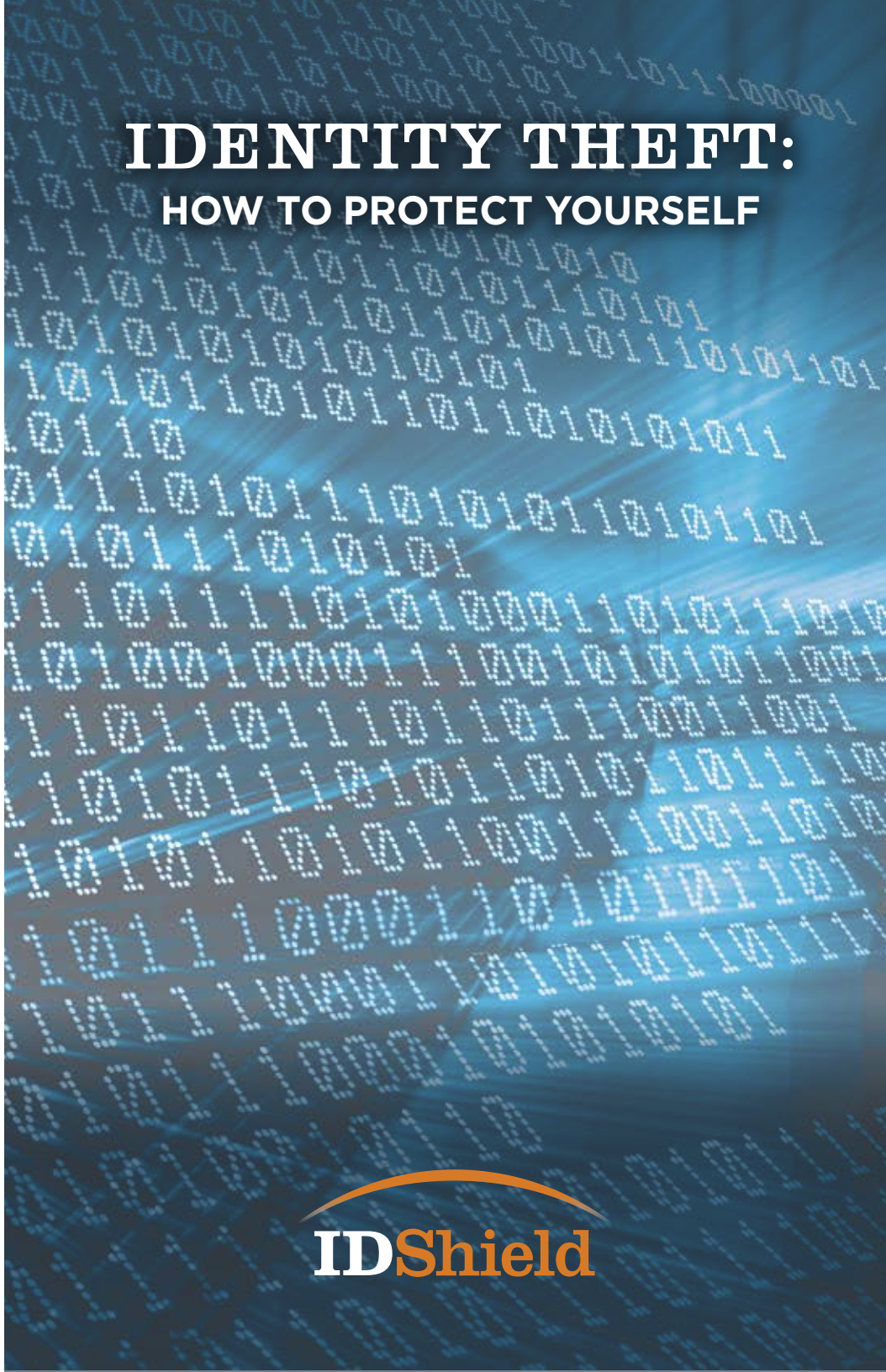
IDShield

How To Protect Yourself

For more information, call your independent associate:



So What is Identity Theft?

"Identity Theft". We hear about it on the news and see posts on social media about identities being stolen, data breaches and much more. But, what does all of that really mean? Most of us assume we're not at risk, we keep an eye on our credit card and bank accounts, so that should be enough, right? Maybe or maybe not.

Definition and Statistics

Identity theft is the fraudulent acquisition of key pieces of personal information, such as Social Security or driver's license numbers, in order to impersonate someone else. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials.

- It's more than just stealing money or hurting your credit score. Criminals would love YOUR money, but really want access to the HUGE amounts of money from the federal and state governments and large corporations.
- Identity theft has been the FTC's top complaint for the last 15 years
- In 2013, 16.6 million people were victims of one or more incidents of identity theft, resulting in $24.7 billion in direct and indirect losses. Of those, 6 million reported emotional distress from their identity theft.
- The lost productivity from employee absenteeism and presenteeism can cost the U.S. economy upwards of $227 Billion in a year.

It's more than just stolen credit cards or bank account information.

Personally Identifiable Information (PII) Identity Theft - theft of someone's SSN, name, address, or a combination of personal information to do any number of fraudulent activities. These could include setting up utilities (electricity, cable, cell phone, etc), obtaining a passport, and others.

Financial Identity Theft - using someone's identity to open financial accounts, obtain loans or obtain new credit/debit cards. This also refers to when a thief steals a credit card or bank account number, and uses it to make fraudulent charges.

Medical Identity Theft - theft of someone's medical insurance number and then use it for their own medical needs.

Social Security Number (Synthetic) Identity Theft - use of a Social Security Number to create a fake credit file. Many times, a thief will combine the information of multiple people (ex: SSN from one person, name and address from another person). The thief then opens new accounts—or commits other types of theft—with this identity.

reports that was related to the identity theft, returning those reports to their pre-theft status.

Additionally the thief used George A's information to open utility accounts with satellite television and internet services providers. And, as with the payday loans, Investigator MacNevin's efforts resulted in the creditor's being made aware of the identity theft, clearing Mr. Allen of responsibility for the debts created and correcting consumer reports tainted by the identity theft.

Case Study: Katherine M.

IDShield member Katherine M. called IDShield for the first time when she received a bill from PayPal. As soon as she stated that she did not have a PayPal account, she was connected to a Kroll licensed private investigator Leslie Moore.

Katherine M. already called PayPal and verified that it was her identity that was used to open the credit card account. Not only did PayPal confirm that the credit card account was associated with her name, birth date and Social Security number, they found a loan that was also associated with her identity.

As Katherine M. recounted these details to Investigator Moore, she also mentioned that she discovered her Social Security number had been used on a fraudulent tax return a couple of months before this incident.

As Investigator Moore began the process of disputing the fraudulent accounts with PayPal, she also helped Katherine M. appropriately respond to the fact that her SSN was on a fraudulent tax return. Prior to calling IDShield, she had only addressed the tax return issue with her accountant. The accountant had not directed Katherine to file an Identity Theft Affidavit with the IRS. Submitting this form will help the IRS understand that she is a victim of identity theft and could help avoid a delay in the processing of her tax return in the following years. The dispute of the two PayPal accounts went about without issue but when subsequent credit reports were reviewed for Katherine M. to verify that the information related to those accounts was removed, one of the reports still reported an inquiry from PayPal. This required yet another form to be submitted to PayPal but Investigator Moore took care of it and kept this frustration from falling on Katherine M..

This is an illustration of how our investigators can help even when the member doesn't realize they need help (as with the tax return issue) and how they save the member from the bulk of the work AND frustration that is part of resolving identity theft issues.

IDShield Case Studies

Case Study: Aaron L

The identity thief that stole IDShield member Aaron L. s identity had expensive taste. The thief succeeded in opening several store credit cards and obtaining more than $20,000 in merchandise. Included among the ill-gotten property was a $4,700 engagement ring . There were $7,000 in charges made with three different cell phone service providers. The thief was using Aaron L.'s identity in ways that he was too responsible to use it himself.

Once he contacted IDShield, he was put in touch with Kroll licensed private investigator Toney, and the process of restoring his identity to what it was prior to the identity theft taking place began.

The thief was fairly bold. At one point, apparently dissatisfied with the credit limit he/she obtained with a retailer that sold music equipment, the thief requested a line of credit increase! That was denied by the creditor; likely because of the flurry of credit applications the thief was submitting using Aaron L.'s identity. In the end, there were 13 attempts to obtain credit, many of which were successful. The thief really "went for it," applying for financing with BMW and Harley Davidson dealerships among more traditional retail credit cards.

The Investigator worked with Aaron L.'s and the creditors to undo the damage done by the thief. The outcome was resolution of all the issues—the creditors, after receiving disputes from Investigator Toney, determined that Levy did not authorize the action taken in his name and he was not held responsible for any of the debt created by the fraud.

Case Study: George A.

Let's begin with the outcome: Kroll's licensed private investigator MacNevin, opened and closed 24 issues while restoring IDShield member, George A's identity.

The 24 issues represent the creditors, collection agencies and consumer reporting agencies that Investigator MacNevin had to contact and re-contact on George A.'s behalf until all the damage done by the identity thief was resolved.

The identity thief used George A's personal identifiers to apply for and in some cases obtain personal loans. One of the personal loans was reportedly obtained to cover $1,000 in medical expenses. However, there were no signs of medical identity theft having occurred. The loans applied for were "quick-cash" or payday loans. This sort of activity doesn't usually appear on the traditional credit reports. This prompted Investigator MacNevin to order and review the consumer reports that might reflect such actions. There are several. She then disputed all data on those

Child Identity Theft - Most children do not have a credit history and the national credit reporting agencies do not knowingly maintain credit files on minors. Because of this, it there is no credit file to monitor for a minor. However, a thief can steal a child's Social Security number and information for fraudulent activities.

Criminal Identity Theft - using a stolen identity while committing crimes or when identifying self during arrest. If a thief is cited or arrested, they can use the stolen ID which causes a criminal record to be created in the victim's name. This could be as small as a traffic violation, or as large as a felony arrest.

Deceased (Zombie) Identity Theft- using a deceased person's information (name, SSN, etc) to open loans, credit cards, or other fraudulent activity.

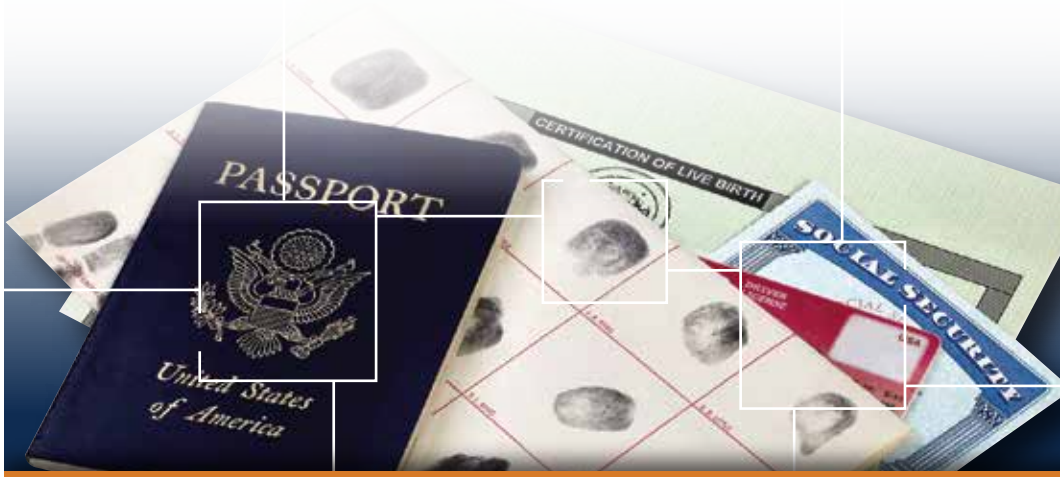
Tax Identity Theft - theft of your social security number to file a fraudulent tax return to obtain a refund.

Government Benefits Identity Theft – using a stolen identity to apply for government benefits such as disability, food stamps, unemployment and even disaster aid.

Employment-related identity theft – using a stolen identity, especially a SSN, to obtain employment.

With so many types of identity theft, that means your personally identifiable information is at risk.

Examples: SSN, name, DOB, email, phone number, address, tax ID, insurance numbers, user names/passwords, credit cards, checks, driver's license number, passport number



Your Personally Identifiable Information Is At Risk.

You have to protect yourself and your information against identity theft. How? Here are a few tips:

Use Strong (And Different) Passwords

- Be careful when choosing a password. Make sure it's something that would not be easy for someone to guess with limited information about you (like what you can find on social media). Things like your school, pet's name, date of birth are easy for thieves to figure out.
- Make sure you use a different password for different accounts. Using the same password for multiple accounts puts all of those accounts at more risk. If there is a data breach or if a thief breaks into one account, many of them will try that same username/password combination other places to see what else they can get access to.

Stop Before You Share

- If you are asked for sensitive information, such as a Social Security Number, ask why it is needed and what systems are in place to protect it.
- Be wary of sharing personal information over the phone, especially if you've received an unsolicited call (even if you do regular business with the organization).

Watch The Wi-Fi

- A thief can sit near a popular Wi-Fi location such as a coffee shop and set up a fake hotspot. Any unprotected data sent over a fake Wi-Fi network can be saved to the thief's computer.
- Use a virtual private network (VPN) connection whenever possible. need more help in protecting our identity.

Have An Identity Protection Service

Having an identity protection service can monitor information you don't have time to monitor in places you can't see, and will help you in the unfortunate event your identity is stolen.

IDShield

With over 170 identity protection service providers, not all are equal, so when selecting a protection service, consumers should look for services that offer internet monitoring, credit monitoring and restoration.

So why IDShield?

IDShield offers one of the most comprehensive products on the market for protecting and restoring your identity.

- **We monitor what matters** - If your name is on it, we're monitoring it. Your Social Security number, emails, phone numbers, driver's license, passport, credit cards, bank accounts and more – we watch over everything connected to you, leaving nothing about protecting your identity to chance.
- **We're here to help** - You have unlimited access to a Kroll licensed private investigator to answer any questions and walk you through all the steps you can take to protect yourself. We're here to help, no matter what.
- **We restore your identity** - In the event of a compromise, your personal licensed private investigator will work to uncover evidence, restore your identity, and clear your record back to it's pre-theft status.