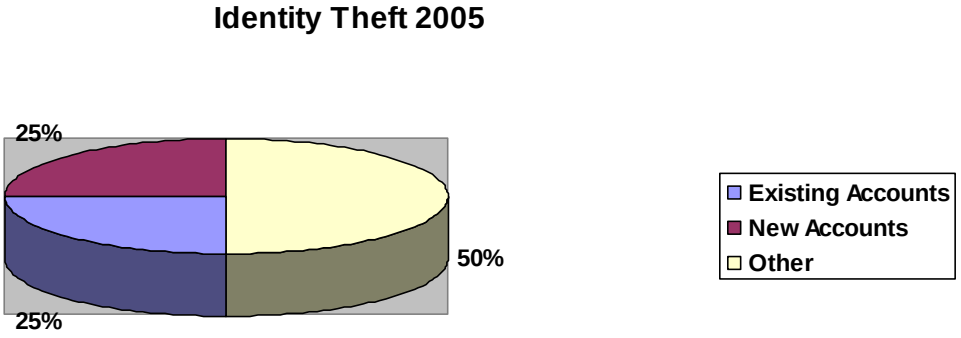
Identity Theft:
More than Account Fraud

What Everyone Should Know

Joseph Campana, Ph.D.
J. Campana & Associates
Madison, WI

www.JCampana.com
608-241-3500

"Identity Theft." What comes to mind? Credit card and bank account fraud of existing accounts? The Privacy Rights Clearing House reported in 2005 approximately 50% of all identity thefts reports were related to credit cards, bank accounts and loans. However, only half related to existing accounts. That means 25% of credit, bank account and loan fraud is on new accounts. Victims of new account fraud may not find out about until it becomes more than just a financial problem for them. The remaining 50% of identity theft reports are non-financial. For example, obtaining utilities, employment, government benefits, government identification (driver license, passport, etc), medical care, housing, insurance, securities and investments, child support, and committing crimes in the victim's name. This means 75% of identity theft goes undetected unless the victim was proactive about detecting the fraud. Proactive means continually monitoring your identities and knowing what to look for.



Many experts, including this author, believe there is a prevalent "It can happen to me" syndrome in North America. This syndrome is thought to originate from the frequent media coverage of existing credit card and bank account fraud, and institutions suggesting how easy existing account fraud is to fix. Because awareness is narrowly focused on existing account fraud, many people believe a financial institution or advocacy group, for example, the FTC, State, law enforcement or other groups, will fully resolve their identity theft issues for them.

Financial fraud from identity theft is just the tip of the growing "Identity Theft" iceberg. What lies below the familiar "existing account fraud" tip of the iceberg?

Take Marie, who I unexpectedly interviewed by telephone while writing this article. She had her checkbook stolen from her purse as she stood in line at the checkout of a retail store late last year. Although she reported her checkbook stolen the following day and the retailer recorded the thief on a surveillance camera, she has spent the last six months trying to clear up the situation with the financial institution; a phone company because of hundreds of dollars in unauthorized long distance calls made to Canada; and the misuse of her husband's driver license number. That stolen checkbook resulted in other identity fraud. Marie is unsure of how the thieves used her checking information to access long distance services and her husband's DMV identity. She still hasn't checked her credit reports to see if there are any other clues of further misuse of her and her husband's identities. While Marie says the detective involved has been helpful, he's swamped handling the identity theft reports of thousands of victims in the Dallas-Fort Worth Area, ranked fourth for identity theft in the U.S. The detective told Marie she is going to need to hire an attorney to address some of the more complex issues. Marie who has been battling

cancer deals with the emotional and financial stress of resolving her family's identity theft crisis on top of the side effects of medication, medical treatment, and additional family expenses resulting the treatment of her cancer. In a sense, she's battling two cancers -- physical and identity.

Why the story? I've heard stories like this hundreds of times during the past few years. I've also heard, many say, "I had my identity stolen, its no big deal, I called the credit card company and they removed the charge and issued a new card." Let's distinguish fraud from identity theft.

Identity theft is when someone steals you (and not your credit card number!). A thief can use any one of your identities to their benefit. In addition to profiting through financial fraud, thieves also profit by selling your identities, often to buy drugs. Your identities can be sold and misused by other criminals, con-artists, terrorists, and even by generally law-abiding people who are in desperate need of a new and specific identity. These scoundrels will use one or more of your identities to their benefit, and by doing so they will blemish or destroy your good name and credibility. In most cases you won't find out for months or even years after the misuse of your identity, if at all. While these different types of identity impersonations can cost victims thousands in lost time and financial losses and expenses; victims of identity impersonation claim the crimes cost them millions more in their emotional stress and frustration bank account.

Which identities are at risk? Your financial identity is the obvious one. You also have other identities, for example: character, education, employment, insurance, medical, motor vehicle, retirement, social security and even an armed services/veteran or business identity.

Who wants your identity? Your identity can be sold and bartered by crooks to commit fraud and crimes including: financial, employment, insurance, criminal, terrorist, tax, internet, phone, utility, rental and any scam that they can conceive. Pick up a newspaper; turn to the identity theft section, where you can read about a new twist on identity theft almost daily.

Although unauthorized credit card and bank account transactions are included in with identity theft statistics (25% of all reports); critics suggest this common and often easily resolved type of financial fraud is not identity theft. What is it? It's simply existing bank and credit card fraud. The account numbers are being used fraudulently, not the victim's identity. A few years ago it was called bank and credit card fraud, and calling it identity theft today appears to be causing a misunderstanding as to what identity theft really is.

While the financial services industry rightfully makes an effort to maintain consumer confidence in their security and privacy practices; the message people have been receiving is that identity theft isn't a problem. For example, the many people will bluntly state, I am not concerned about identity theft because I don't use credit cards.

Most often, your identity is compromised by a person who obtains your personal identifiers. Your key person identifiers are simply your name, birth date and social security number (not your bank account number or credit card number). These three identifiers can be sufficient for an imposter to establish an identity for their benefit.

Financial Identity Theft. "New account fraud" occurs when these three personal identifiers are used to establish credit, bank accounts, and take out loans and new credit cards. Those new credit cards and loans are issued to your impersonator at their mailing address; not to you – at least not to the real you. You won't be notified when your impersonator uses, misuses, or misses payments because your impersonator used their address or more commonly a temporary post office box or fictitious address for financial gain by using your name.

The best way to catch this potentially devastating financial fraud is to review your credit reports regularly to look for clues that you may have become a victim. Those clues include change of address, credit inquiries, new loans, new credit cards, derogatories (late payments), collections, liens, and bankruptcy. The earlier you detect the clue, the less damage to you. For example, identifying a change of address or credit inquiry within a few days of a change reported to the credit reporting agency (CRA) could put you in the position to notify the financial institution before they issue credit or a loan to the imposter. When you get the clue that early in the fraud process, you can halt the fraud and it may even be possible to catch the thief.

The importance of checking your credit reports regularly and frequently is the reason why continuous credit monitoring services have become so popular. With credit monitoring services, instead of you checking your credit reports annually or even monthly, the CRA notifies you whenever a change is entered into your credit report.

Non-Financial Identity Theft -- The Other 50%. What if someone with a "high-risk identity" can't get auto or health insurance, a driver's license, medical care, a cell phone or other utilities, or even a job? Because of the proliferation of identity theft crimes, it is not uncommon for a person who is desperate for insurance or a job to use the identity of another to fulfill their basic survival needs. These desperate people use identities impersonally without considering the violation of privacy and identity rape they are committing on you. They don't consider the financial and emotional stress imposed on the victims or businesses by their crimes of desperation.

Why do seemingly law-abiding people commit identity theft? It's easy, it hard to get caught, and in certain situations, the law says no crime was committed. Suppose you couldn't get affordable health insurance for your family, or you couldn't get auto insurance? By using the identity of another you could get the insurance you need to protect and to provide for you and you family. You're going to pay the premium, so no one is going to get hurt, and in some circumstances it's not even considered a crime! Would you do it if you were desperate, *and you believed no one would get hurt and you wouldn't get caught?*

Other criminals purposefully and maliciously use identities of others to commit crimes, defraud government benefit programs and retirement funds, and conspire and perform acts of terrorism.

A few examples of the consequences of "Non-Financial" identity theft crimes are:

- Increased insurance rates or denial of insurance because some higher risk imposter has applied for, has been issued, or has been denied auto, health, or other insurance in your name.

- You are denied utility or phone service because records show you owe on past services in several other states;

- You are penalized by the IRS for thousands or even millions of dollars in unreported wages earned in Texas, Arizona and California;

- You are detained by customs agents or airport security coming back from a vacation in the Bahamas because your name is flagged as a criminal or a suspected terrorist;

- Debt collectors are harassing you for past due bills incurred by financial ID thieves in several states;

- You are arrested at your home, at work, or in a routine traffic stop because one or more Federal law enforcement agencies have issued a warrant for your arrest for crimes that someone else committed in your name.

- You are medically mistreated in an emergency room situation based on a medical history that reflects the treatment to your medical impersonator;

- You are denied tenancy or a mortgage because your records show you are a high risk;

- You learn that you took an early retirement and that certain Federal benefits have already been drawn on by an impersonator, and now you have to prove it wasn't you;

- You learned you sold your winter condo in Arizona when you arrive and the new legal owner opens the door as you are fumbling to get your key into the changed lock;

- After several months or years of unsuccessful job hunting, you learn that you have been denied employment all this time because you have a criminal record showing felonies committed in Oregon and Idaho;

- Your 3-year old son ran up a debt of $50,000, and collection agencies are calling your home;

- You are denied unemployment insurance because you are also employed in Arizona and California.

- You find that a deceased parent is working in Chicago, when you receive an IRS notice in their name for penalties on unreported earnings.

These are some of the other faces of identity theft. These are a few true grit examples, which illustrate that identity theft situations often occur in multiple jurisdictions. Multi-jurisdictional issues add to the complexity of resolving the crime and proving that you are the victim.

There are no credit monitoring services, no banking or credit card guarantees, and no identity theft insurance that are going solve these types of identity theft issues and consequences. Some of these identity theft situations can take years to mitigate and more often than not they cannot be completely resolved even after victims spend several hundred hours and thousands of dollars trying to get back their good name.

Identity theft insurance and advocacy or "resolution" services leave the emotionally distraught victim frustrated by having to restore their good name. Identity resolution services are like having a coach cheer you on as you dedicate and prepare yourself to run a marathon with no prior experience. It's still your blood, sweat, and tears to clear your name, and even if you finish, it doesn't mean you won.

Identity "restoration" services are also available, which cover all types of identity fraud. Restoration services may provide licensed expert fraud investigators to perform all the critical tasks and paperwork to restore your identity to where it was in before it was compromised. But even these comprehensive services can leave gaps in the restoration process. You may need to hire an attorney to address general legal issues; lawsuits against you from creditors; Federal audits and inquiries; to restore your character identity by expunging crimes on your court records; and even to restore your medical identity by expunging notations and medical services from your medical history. Fixing erroneous court and medical records seems straightforward; however, clearing your character identity as well as clearing your medical identity are perhaps the most critical and most difficult of all, which is why it imperative to have experienced experts and legal counsel who can do that for you.

The financial services industry and professionals can go beyond educating employees and customers about "existing account" fraud, by providing the bigger picture of identity theft – it's much more, and much more devastating to the victims. The other types of identity theft indirectly affect or result in financial fraud or affect personal finances of your employees, your customers, and ultimately your bottom line.

About the Author

Joseph Campana, Ph.D. is a certified identity theft risk management specialist (CITRMS) accredited by the Institute of Consumer Financial Education.

J. Campana & Associates provides consultation, training, and risk management solutions to businesses, employers, and employees. Dr. Campana is a frequent seminar speaker on identity theft and has appeared on radio and TV. He founded the LegalEase Group, Madison, Wisconsin in 1998, which provides insurance continuing education on legal expense insurance and identity theft topics. He has also been affiliated as an executive and trainer with a publicly –traded international services firm that provides identity theft and legal risk management insurance to employers, businesses, and families nationwide and in Canada. Dr. Campana may be contacted by telephone: 608-241-3500 or by email: campana@JCampana.com. The J. Campana & Associates website is: www.JCampana.com.