A McCann E-Investigations White Paper
www.einvestigations.com
(800) 713-7670

Victims of Identity Theft Should Consider Hiring a Private Investigator

April 9, 2012

Summary:
Co-written by an 18 year veteran in law enforcement and a subject matter expert in private investigations and security, this paper explores the complexities of identity theft investigations and focuses on the steps that a victim must take to assist law enforcement in the investigation. This includes the use of services provided by a private investigative firm with computer forensics background who can examine devices for evidence of network breach and safeguard potential future breaches. The information gathered in the digital forensic examination can provide law enforcement with the evidence they need to track down the perpetrator

The Benefits of Private Investigators in Identity Theft Investigations

George Mason is a successful 36 year old midlevel manager at an accounting firm. He, his wife Judy, and their two kids live in a nice house in an affluent suburb and enjoy all the trappings that an upper income lifestyle provides. Golf for him, ladies luncheons for her and gymnastics for the kids. George is moderately computer savvy, and takes pride in the fact that he efficiently takes care of all of his bills and taxes online and on time. While the family has some credit cards, they aren't ever anywhere near maxed out. The kids' college funds are continuing to grow, despite the rough markets. Life is great for George and his family.

George is at work checking over month end close documents one afternoon when he receives a phone call from Judy. It seems Judy received a perplexing letter in the mail, and wanted to know if George could make heads or tails of it. She tells him the letter was a credit statement from a computer company saying he had purchased a $1,000 gift card. She says the thing that made her question the bill was the fact the card had been shipped to a different city. George tells her he doesn't know anything about it, and that he will call the computer company and find out what's going on. Judy then asks him if he had purchased jewelry lately. She goes on to tell him that she had received a bill a couple of weeks prior for a $6,000 purchase from a large jewelry chain, but that since their anniversary was coming up soon she had just assumed he was trying to surprise her. George, knowing he had yet to shop for their anniversary, immediately became concerned and told his wife that he was calling the bank.

After waiting on hold for twenty minutes and fighting with the automated answering system, he finally gets through to a live person. His relief is audible when he finds out their checking account has the correct balance. Unfortunately, his relief turns to terror when he discovers their savings account shows a balance of only $250, when it should be about $35,000. He demands to know what happened to the funds and turns clammy and sick to his stomach when he is told that he had initiated an electronic funds transfer two weeks prior. The customer service representative tells him that the savings account funds were moved the same day as the two college funds. $78,000 gone like a wispy puff of smoke. George now realizes his world has forever been changed, and that he is a victim of Identity Theft.

After receiving the sickening news, George leaves the office and drives directly home. On the drive he asks himself a lot of questions: How could this have happened? How much has

really been taken? How do I get my money back? What do I do now? He already canceled all of their credit cards and debit cards during the phone call with the bank, and they told him to call the police as soon as possible. As he pulls into his driveway, George dials the local police and tells the dispatcher that he thinks his identity has been stolen and he needed to make a report.

George goes into the house to find his wife hunched over the kitchen table with papers all over the table. As he walks up to her, he hears her sobbing and sees damp spots from tears dotting the bank statements in front of her. He tells her that everything is going to be OK, even though he doesn't' yet know for himself if that's true or not. He sits next to her and asks her if there have been any other unusual letters or credit statements in the mail. Before she can answer, the doorbell rings. George opens the door and greets the officer standing on their porch. He explains the events of the day to the officer, who listens intently and takes notes. At the end of the interview, the officer gives George an incident number and tells him that an investigator will be contacting him in the next few weeks. As the officer turns to leave, George asks her what he should do in the mean-time? The officer's only advice is for him to contact the credit reporting agencies and let them know his identity has been compromised.

Every year in the United States, 15 million people are victims of Identity Theft. For the victim, it's important to understand that Identity Theft is a general term for a multitude of different crimes. Among them are credit card and debit card abuse, checking and savings account fraud, investment account fraud, tax fraud, and mortgage fraud. Due to the varied nature of the crimes, once a person's identity is compromised, the damage can continue for months or years.

Of all property crimes, Identity Theft is the most challenging for all parties involved. For the victim it means putting a stop to the active misuse of their identity, identifying the extent of the damage, dealing with the bureaucracies of the defrauded creditors, the banking system and law enforcement, attempted recovery of stolen assets, and the most daunting task of reclaiming of their identity. For the banking system it means dealing with customer anger, determining if the source of the identity theft was a banking institution, determining if this customer's problem is isolated or part of a wider scheme, detecting loopholes in banking policies and internal controls, and finally assisting law enforcement with successful prosecution. For law enforcement it means coordinating with the victim and other entities to obtain all of the evidence, determining (if possible) the means by which the victim's identity was compromised, identifying potential suspects, tying the evidence to any suspects for prosecution, documenting the case for

trial, locating and arresting the suspect, and then assisting the District Attorney's Office in the successful prosecution.

The focus of this study will be predominantly the steps that the victim of identity theft must take to weather the storm and as quickly as possible put their personal and financial lives back in order. The banking and law enforcement angles will also be touched upon to provide context for why being a victim of identity theft is such a massive challenge. The additional angle of the use of a private security firm will be explored to show how they can effectively assist the victim of identity theft from both becoming a victim in the first place, as well as being an invaluable asset in post-victimization response.

For the victim, the speed and effectiveness of stopping the active misuse of their identity is probably the single most important factor in determining how catastrophic the damage is going to be in the long run. Victims who don't take on this mantle quickly enough can potentially be dealing with repeated episodes of identity theft for months or even years. This is due predominantly to the free flowing nature of information on the internet. Identity thieves are sometimes the most computer savvy criminals in the spectrum. The reason for the more intelligent nature of these thieves is up for debate, but many believe it is because the potential reward (tens if not hundreds of thousands of dollars), is much greater than the likely penalties of probation or extremely short jail sentences should they be caught. The single most effective way of stopping the active misuse of identity is working with the credit reporting agencies to limit access to the victim's credit. The identity theft addendum, attached to this report, provides all of the resources victims need to address the steps necessary to limit the extent of identity theft damage.

Dealing with the bureaucracies of defrauded creditors, the banks, and law enforcement are a significant source of frustration for all victims of identity theft. Once of the best ways to get a handle on these institutions is establishing a log of any and all contacts. This log should include the date/time of the contact, the person who was speaking on behalf of the entity, and a brief summary of the contact. Keeping a log will greatly improve the victim's ability to keep track of what's supposed to be done, as opposed to what's actually been done, as well as enable the victim to hold people accountable in the future, if necessary. After wading through the maze of bureaucracies, recovery of stolen assets becomes the next priority.

Recovery of stolen assets in identity theft, unlike other types of theft, is normally a matter of the bank absorbing the loss on behalf of the victim. Banks and creditors are usually

very quick and willing to correct fraudulent transactions. The exception being when victims sometimes divulge information on their identity through social engineering on the part of the suspect. Normally this occurs with elderly victims being cold called by suspects and then tricked into providing personal identifiers. In these cases, creditors sometimes refuse to refund the fraud since they consider it negligence on the part of the victim. In these instances, the only recourse is for the victim to seek restitution from any suspects prosecuted for the theft. The final victim consideration in identity theft cases is the reclaiming of the victim's identity.

The process of reclaiming their identity by the victim is really the legacy task in all identity theft cases. This process can take months or even years depending on the severity of the theft, and requires constant vigilance on the part of the victim. Most identity theft victims will have to regularly check their credit reports for at least a year or two to make sure new fraudulent entries don't appear on their reports.

While daunting and time consuming, victims of identity theft can usually reclaim their identities and lives within a reasonable amount of time in most cases. The scariest aspect though is the fact that once a person has been the victim of identity theft, it is often only a matter of time before they are victimized again. Once again, this is due to the free-flowing nature of information in our internet culture.

So what does someone do to prevent themselves from being a victim in the first place, as well as prevent themselves from being victimized again in the future? Let's check back in with George Mason and see what he does…

Immediately after making his initial police report, George Mason contacts the credit reporting agencies and puts a fraud alert on his credit file. He also orders copies of all of his credit reports to check for any other unauthorized accounts. Once they arrive in the mail he is shocked to find there have been nine fraudulent accounts opened in his name. By now it has been two weeks since he made his police report and he still hasn't heard from the police investigator. Frustrated at the task of figuring out how this all happened and what to do next, he pulls a business card out of his wallet that was given to him by his boss. The business card is for a local security and investigative firm his boss had used in a recent corporate embezzlement case their business was involved in. At the time, George didn't realize that a private investigative firm could help in situations like his, but feeling overwhelmed and somewhat helpless he gives them a call.

Mike Schwartz, an investigator with the firm, comes to George's house the very next day. He tells George that they can not only help him deal with his end of the identity theft, but that by using their services it will decrease his chances of being victimized again, as well as increasing the likelihood of a successful prosecution by the police. While there, Mr. Schwartz scans the Mason's computer network and finds several potential security gaps. Mr. Schwartz tells Mr. Mason that he needs to take their computers back to their lab to try to figure out if that was the source of the security breach. He also makes redacted copies of the credit reports to assist in compiling the investigative report that will assist in the police investigation. Hoping this was a good decision, George watches Mr. Schwartz cart their desktop and laptop computers to his car.

By the third week after making the police report, George is beginning to get a bit frustrated. He has left several messages with the police without a returned phone call. Mr. Schwartz warned him during their first meeting that many times these cases don't get a lot of traction with the police without a substantial amount of "foot work" by the victim. George is feeling somewhat better though because the investigative firm returned their computers two days after taking them. When they were returned, Mr. Schwartz brought his own computer in their house and adjusted the settings on their network to patch the security holes. He also told him that new software had been installed on their systems to better secure their data from both viruses and unauthorized intrusion.

It had been roughly a week after hiring the investigative firm when Mr. Schwartz came over with the report they had compiled on the identity theft. The report showed that the likely source of the identity breach was a piece of spyware and a key logger on his desktop computer. The report also detailed each fraudulent account and transaction, as well as information to help the police track down a suspect. This information included IP addresses, transaction details, and associated addresses. Mr. Schwartz told George that with this report the police should be able to find out who it was that stole his identity. Armed with the investigative report in hand, George went to the local police station and sat down with Investigator Jason Shipley to discuss his case. Needless to say, Investigator Shipley was surprised and impressed with the report and told Mr. Mason that he would look into his case now that there were potential leads to follow.

According to the American Bankers Association (ABA), in 2010 there was almost nine-hundred million dollars in check fraud alone. This doesn't account for the untold amount identity thieves stole in the myriad of other ways they victimize people. Local police agencies

are routinely understaffed and underfunded and often don't have the resources to give every case of identity theft the attention they deserve. This is a matter of practical use of resources not lack of desire to solve crimes by police. There are simply not enough man-hours to take an identity theft case with no leads and run it down to its conclusion unassisted. This is where active participation by the victim makes all the difference.

The first step the investigator must do is collect the evidence of the crime. In identity theft cases this is usually credit reports, letters from creditors or banks, victim bank statements, fraudulent transaction details, delivery receipts, cancelled checks, etc. Gathering all of these documents unfortunately falls on the shoulders of the victim. This process can be extremely time consuming and frustrating for the victim, which is why some people choose to hire private investigative firms to do all of the "leg work" for them.

Once the investigator collects all of the supporting documents, he must then get grand jury subpoenas to compel the companies and banks to turn over all documents related to the fraudulent transactions. This is often where information such as IP addresses becomes invaluable. If the victim hasn't obtained this information already then the officer must first subpoena companies just to get the IP addresses and then turn around and subpoena the internet provider for IP address subscriber information. It can take over a month to get information requested in a subpoena so any step that the victim can save the police will save valuable time in the investigation.

IP address subscriber information is basically who the internet service provider has assigned a particular IP address to at a specific date, time, and time zone. Since most residential IP addresses are assigned dynamically, multiple people may be assigned the same address on any given day which is why time and time zone are very important. Once the police investigator gets the subpoena response on the IP address, he knows from which address (or cell phone number if it's an IP address assigned to a cell phone data plan) the fraudulent transactions were made. This is primary source of potential suspect information for online identity theft. Now that the investigator knows WHERE the suspect resides, identifying the specific suspect from that address becomes the next task.

Determining the identity of the specific suspect often takes persistence on the part of the investigator. This normally starts by determining the owner of the residence where the IP address was assigned at the time of the fraudulent transaction. Once the owner is determined, the investigator will find out the identity of every person living at the location and who there

already has a criminal record. Most of the time identity thieves already have a criminal history, with a lot of them having previous arrests on fraud related crimes. Once the names of potential suspects are discovered, the investigator will obtain photographs of the suspects from either driver's license photos, or criminal mug shots and then the investigator will put together a photo array.

For physical items purchased using fraudulently obtained credit, usually the suspect will have the item shipped somewhere where he doesn't live but that the suspect has access to when nobody else is there. Normally this will be a vacant house, closed business, or church during the work week. The suspect will wait outside the location for the delivery to be made and pose as a legitimate recipient of the package for the location. This is why delivery information supplied from where the fraudulently obtained item was purchased is vital to the investigation. Often delivery drivers will remember specific deliveries and be able to identify suspects if shown a photo array in a timely manner. If the delivery driver is able to pick out the suspect derived from the IP address location, then the investigator should have enough evidence to charge the suspect.

For account take over schemes using victim identifiers, suspects will trick financial institutions into allowing them to electronically move money out of victim accounts into accounts belonging to the suspect or associates of the suspect. All electronic fund transfers (EFTs) leave traceable information with the financial institution on where the funds were transferred to. Once the investigator gets the routing number and account number of the receiving bank, he can then subpoena the bank records for account owner information as well as video associated with withdrawals of stolen funds. With this information the investigator should have enough information to charge the suspect. It should be noted that the actual perpetrators of the identity theft are often not the person who receives the funds in the transfers. Sometimes the original suspect will convince another person to allow the funds to go into their accounts. The original suspect will then let this person keep a small portion of the funds in exchange for giving the rest of the funds to them. This new suspect will almost always inform on the original suspect when they realize they are being charged with a crime.

Every identity theft case is different and this only provides a snap shot of one typical example of this type of crime. It does represent the many steps involved and the days and months it can take to track down suspects. Considering most major cities get dozens (and in some cases hundreds) of these cases each month, it stands to reason that the more a victim can

do to assist the police in their investigation, the more likely their case will be brought to a satisfactory end.

Let's check in on George Mason one last time. It's been three months since George Mason realized his identity had been stolen. His credit is still locked down and he plans on checking it twice a year for the foreseeable future. All of the fraudulently obtained credit accounts have been closed and there have been no reports of any additional criminal activity. His savings account has been refunded to its previous balance, and the kids college accounts are where there were before all of this mess. Life has basically returned to normal. Mr. Schwartz told him it could be three or four months before he hears any news from the police and has kept in touch with him during this time to check and be sure that his family was recovering from the security breach. On a Friday afternoon just after getting home from work he gets a strange phone call from out of state. His gut jumps into his throat at the prospect of this being news of a new fraudulent account being reported to him. It takes a moment on the phone to realize the caller is an officer a different state telling him that the suspect in his case had been arrested that morning. He goes on to tell him that the suspect is gang member and also wanted by the FBI and that it was his case and the fact that he had so complete of report in his file that all of the cases were able to be tied together to this single individual.

Identity Theft is a crime that has been around for a long time, but has only in recent decades gotten out of control. Looking toward the future, it seems that this crime will continue to be on the forefront of expanding criminal enterprise. Only through vigilance of consumers, banking institutions, businesses, law enforcement, courts, and legislators will this epidemic be contained and maybe one day turned back. In the future there will also likely be a larger role played by private investigative firms, who will take up some of the burdens that ever shrinking budgets have placed on our public institutions.

Identity Theft Victim Resources

The major credit reporting agencies are:

Equifax:

www.equifax.com

(800) 685-1111

Experian (Formerly TRW):

www.experian.com

(888) 397-3742

Trans Union:

fraud.transunion.com

(800) 680-7289

When contacting the credit reporting agencies there are two requests you can make. First there is a 90 Day Fraud Alert (Active Duty Alert for Active Duty Military Personnel). This will prevent anyone from obtaining credit using your personal information without the additional security steps established by the credit reporting agencies. This service is free for identity theft victims and may be extended, if necessary. This request need only be made to one of the agencies, as they share the information with one another. The other request is called a Security Freeze. A Security Freeze operates in the same manner as the 90 Day Fraud Alert but can be temporarily or permanently lifted by the requestor. Most states have laws mandating a Security Freeze be free of charge for victims of identity theft (except for Arkansas, Colorado, and Mississippi). Unlike the 90 Day Fraud Alert, a Security Freeze must be placed with each credit reporting agency individually. In most cases you will have to establish, make changes, and cancel a Security Freeze in writing at the following addresses:

Equifax Security Freeze

PO BOX 105788

Atlanta GA 30348

Experian Security Freeze

PO BOX 9554

Allen TX 75013

Trans Union Fraud Victim Assistance
PO BOX 6790
Fullerton CA 92834

The single most effective response by the victim (after contacting law enforcement) is to contact the credit reporting agencies, and notify them that you are a victim. Once the credit reporting agencies are alerted, the extent of additional long-term damage is extremely limited. After that, the focus of the immediate response is one of controlling any potential localized damage. To accomplish this, all banks and legitimate creditors should be contacted and informed that your identity has been compromised. Any accounts where fraud is suspected should be closed immediately. Those entities should note that information in your files and then immediately reissue any debit or credit cards, as well as notify you of any suspicious activity on any of your accounts. Finally, all victims of identity theft should make a complaint with the Federal Trade Commission (FTC). http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

About the Authors:

John D. Shirley is a third generation peace officer and 18-year veteran of law enforcement in Houston, Texas. After cutting his teeth as a patrol officer on the streets of North Houston he went on to do crime analysis, police policy writing, internal investigations, and homicide investigations. He is now an Investigative Sergeant in his department's Financial Crimes Unit. John is also the State Chapter President of the Oath Keepers organization and lives in North Houston along with his teenage son.

Daniel Weiss is Managing Partner at McCann Investigations, a Texas-based private investigations firm. McCann Investigations focuses on hybrid investigations encompassing computer forensics and traditional private investigative practices (surveillance, undercover work and background checks). Daniel began his career in the security industry while in graduate school at Northeastern University, where he worked at Wolpole State Prison in Massachusetts. He left the public sector and entered the private security sector. During the past 15 years, he has worked for Wells Fargo and Chubb, and has started three successful private sector security firms

EPS Security, GCS, and Infrastruct Security. Daniel has been interviewed as a subject matter expert on security by ABC, NBC, CBS, Security Director News, SDM, and Security System News. In addition Mr. Weiss has been featured in the Houston Chronicle and Houston Business Journal.