Identity Theft – Befofe and After It Happens

Michael Fetick, 84270

Coleman University

**Identity Theft – Before and After It Happens**

**Identity Theft – Before it happens**

Before the cybercrime of Identity Theft happens, individuals can take security precautions to thwart an attack (sometimes called an incident). Sometimes an individual has the role as either a potential consumer, potential employee, or potential investor and is interested in investigating a business contact before [potentially] doing business. This research paper covers both, steps for precautions and investigations that an individual can do, to prevent or elude the risk of Identity Theft.

The front-line of the fight lies with the potential and real victims of the crime, which are usually common, citizen individuals. The individual has the tasks to 1) research information about the crime and precautions to take 2) perform steps to take those precautions. It is best to find the resources from the top to bottom but the individual must interact with resources at the lowest level to deal effectively with the problem, from the bottom-up.

The Federal Trade Commission offers a one-stop resource for consumer information on how to report and recover from Identity Theft at the website IdentityTheft.gov (Federal Trade Commission (FTC), 2015). The FTC also presents information about scam alerts and what to do about scam in the news (FTC - Scam Alerts - Consumer Information, 2015). There is an interesting Scam Tag: Work-at-Home.

The individual knowledge seeker can do research with a search engine and see the resulting resources. A good start for general Information is the FBI’s National Cyber Security Awareness Month (October) (Federal Bureau of Investigation (FBI), 2015) and internet crime prevention tips (Federal Bureau of Investigation (FBI), 2015). Further detail of attacks describe the Internet Crime Schemes of Phishing and Spoofing to forge or fake internet documents (Internet Crime Complaint Center (IC3) Internet Crime Schemes, 2015).

The Department of Justice (DOJ) presents an abundance of information about Identity Theft and Identity Fraud, common ways it is committed, what the DOJ is doing about it, some examples of recent cases, what an individual can do to avoid it and to mitigate it (Identity Theft CRIMINAL-FRAUD Department of Justice, 2015).

There is an abundance of good information from the State of California, Department of Justice - Office of the Attorney General [Kamala D. Harris] (Identity Theft Information Sheets State of California - Department of Justice - Kamala D. Harris Attorney General, 2015). The best one is, “Top 10 Tips for Identity Theft Protection” which lists: 1) Protect your Social Security number, 2) Fight “phishing” – don’t take the bait, etc.

**Identity Theft – After it happens**

After Identity Theft happens, there is damage control and investigations. The victim of the crime is an individual that is trying to endure through the stress caused by financial loss and/or the addition of insurmountable, erroneous debt. The victim must try to limit the loss (by closing accounts) and submit complaint reports (to initiate investigations). The attack can occur with a long delay before the criminals to commit the crime and thus, be detected. This can make the investigation difficult to determine the cause of the attack and may create a continuing threat.

When financial papers are tampered with or monetary losses are apparent, only then will the individual know they are a victim. Then, they have the enormous tasks of 1) reporting the crime (filing a complaint) [complaining]; 2) closing accounts and changing passwords to limit and reduce the damage, 3) opening new accounts and creating new social security number to resume a functioning, normal life.

The Federal Trade Commission offers a one-stop resource for consumer information on how to report and recover from Identity Theft at the website IdentityTheft.gov (Federal Trade Commission (FTC), 2015). The FTC’s IdentityTheft.gov presents “Warning Signs of Identity Theft” for clues that someone has stolen your information (Warning Signs of Identity Theft - IdentityTheft.gov, 2015). They also present a plan to make it easier to recover from Identity Theft; they tell the individual what to do right away, what to do next, and other steps (Identity Theft Recovery Steps - IdentityTheft.gov, 2015). The crime can be reported through the FTC’s “FTC Complaint Assistant” with multi-page forms to fill out, online (- FTC Complaint Assistant, 2015). It also includes a link to downloadable memorandum with instructions, to be given to your local Law Enforcement Officer.

The individual knowledge seeker can do research with a search engine and see the results for more resources. A good source is the Wiki website for general information, though it is not necessarily the best source for authoritative, accurate, or timely information is well developed (Various Government Agencies, 2015).

The FBI’s Internet Crime Complaint (IC3) investigates cybercrime complaints and may refer the complaint to federal, state, local, or international law enforcement or regulatory agencies (Federal Bureau of Investigation (FBI), 2015). The FBI’s 2014 IC3 Statistics says over 3.1 million complaints were reported to the IC3 since inception (FBI Internet Crime Complaint Center (IC3), 2015).

The Internal Revenue Service (IRS) presents a Taxpayer Guide to Identity Theft at their website (IRS - Taxpayer Guide to Identity Theft, 2015). The IRS refers to terms like tax-related identity theft, employment-related identity theat. I see a fundamental security vulnerability in the IRS W-4 reporting system. The W-4 form contains an individual’s social security number and is required to be reported by the employer, to the IRS. But in cases of legitimate businesses that offer remote-work – they also have to report that information and it can be impossible for an individual to determine if the remote-job offer is legitimate, or is the company a scam?

There is support at the State Government level. For example, at the State of California, Department of Justice - Office of the Attorney General [Kamala D. Harris] there has been a California High Technology Crimes Force strategy since 1998. It is divided through five regional Task Forces to manage the “High Technology Theft Apprehension and Prosecution (HTTAP) Program (State of California, Attorney General - HTTAP Program, 2015). Their focus is to combat identity theft and offer Identity Theft First Aid. Such a case may involve an individual that says, “I am getting calls from debt collectors and creditors on accounts I know are not mine.” An individual affected by Identity Theft can register with the State’s database of victims.

Locally to me, the San Diego County Sheriff’s Department presents a website to report Financial Crimes, such as Identity Theft, Scams, Embezzlement, and Fraud/Forgery (San Diego County Sheriff’s Department - Financial Crimes, 2015).

There are a few national, consumer-advocate organizations, such as Identity Theft resource Center (ITRC) at www.idtheftcenter.org that offers protection tips and no cost assistance (Identity Theft Protection Tips - Protect yourself, 2015). There are businesses that offer identity protection, such as LifeLock, Identity Guard and IdentityForce. They are reviewed and compared by IdentityTheftLabs saying, “Identity Protection – Do I Really Need It (Identity Protection – Do I Really Need It, 2015)?

**Identity Theft – Resources for Prevention / Investigation**

The most effective way to protect against Identity Theft is to integrate the partnerships of legal resources of both efforts, afforded before and after the crime. The war on cybercrime, particularly Identity Theft, is fought by our government’s commission and collaboration of law enforcement agencies at Federal, State, and local levels and assisted by various national and international, consumer-advocate organizations.

At the U.S. Government’s federal level is the Federal Bureau of Investigations (FBI), the Federal Trade Commission (FTC), and the Internal Revenue Service (IRS). At the government’s state level is the State Adjutant General (SAG). At the local government level is the law enforcement of local police and sheriff departments.

Collaboration of these resources is directly supported online with hyperlink references to each other’s website details. Inter-agency collaboration is continuously improving but there are two problems that confront the individual knowledge seeker: 1) too much information is overwhelming (overloaded by multiple functions, value propositions); 2) the lack of essential information where it would be most effective. Collaboration is also indirectly supported online with search engines like Google and Bing. They are readily available to individuals but the sorted order that search results are listed is dependent on many technical variables of search-engine optimization (SEO) and revenue-generation politics.

**Thesis Peer Review**

This thesis paper was reviewed by a peer. The review was acknowledged with the following comment: Wenona Fetick who says, “It seems rather difficult for a person to find the right information while trying to deal with the crisis of having their identity stolen. This is a good research paper.”

# References

*- FTC Complaint Assistant.* (2015, Nov 3). Retrieved from https://www.ftccomplaintassistant.gov/#crnt&panel1-1

FBI Internet Crime Complaint Center (IC3). (2015, Nov 3). *Internet Crime Complaint Center (IC3) Prevention Tips.* Retrieved from IC3 Brochure: http://www.ic3.gov/preventiontips.aspx

Federal Bureau of Investigation (FBI). (2015, Oct 31). Retrieved from FBI — National Cyber Security Awareness Month: https://www.fbi.gov/news/stories/2015/october/national-cyber-security-awareness-month

Federal Bureau of Investigation (FBI). (2015, Nov 3). Retrieved from Internet Crime Complaint Center (IC3) Prevention Tips: http://www.ic3.gov/preventiontips.aspx

Federal Bureau of Investigation (FBI). (2015, Nov 3). *Internet Crime Complaint Center (IC3) Home*. Retrieved from Internet Crime Complaint Center (IC3) File a Complaint: http://www.ic3.gov/default.aspx

Federal Trade Commission (FTC). (2015, Nov 3). *Identity Theft - Consumer Information.* Retrieved from http://www.consumer.ftc.gov/features/feature-0014-identity-theft

*FTC - Scam Alerts - Consumer Information.* (2015, Nov 3). Retrieved from http://www.consumer.ftc.gov/scam-alerts

*Identity Protection – Do I Really Need It.* (2015, Nov 3). Retrieved from http://www.identitytheftlabs.com/identity-protection-plans/

*Identity Theft CRIMINAL-FRAUD Department of Justice.* (2015, Nov 3). Retrieved from http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

*Identity Theft Information Sheets State of California - Department of Justice - Kamala D. Harris Attorney General.* (2015, Nov 3). Retrieved from http://oag.ca.gov/idtheft/information-sheets

*Identity Theft Protection Tips - Protect yourself.* (2015, Nov 3). Retrieved from http://www.idtheftcenter.org/Protect-yourself/id-theft-prevention-tips.html

*Identity Theft Recovery Steps - IdentityTheft.gov.* (2015, Nov 3). Retrieved from https://www.identitytheft.gov/

Internet Crime Complaint Center (IC3) Internet Crime Schemes. (2015, Nov 3). Retrieved from Internet Crime Complaint Center (IC3) Internet Crime Schemes: http://www.ic3.gov/crimeschemes.aspx#item-14

*IRS - Taxpayer Guide to Identity Theft.* (2015, Nov 3). Retrieved from https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft

*San Diego County Sheriff’s Department - Financial Crimes.* (2015, Nov 3). Retrieved from http://www.sdsheriff.net/financial/index.html

*State of California, Attorney General - HTTAP Program.* (2015, Nov 3). Retrieved from http://oag.ca.gov/ecrime/httap

Various Government Agencies. (2015, Nov 3). *4 Ways to Report Fraud - wikiHow*. Retrieved from wikiHow - How to do anything: http://www.wikihow.com/Report-Fraud

*Warning Signs of Identity Theft - IdentityTheft.gov.* (2015, Nov 3). Retrieved from https://www.identitytheft.gov/warning-signs-of-identity-theft.html