

California State University, San Bernardino

**CSUSB ScholarWorks**

---

Theses Digitization Project

John M. Pfau Library

---

2012

## Identity theft: A problem of complex systems or moral panic?

Matthew Timothy Tracy

Follow this and additional works at: <https://scholarworks.lib.csusb.edu/etd-project>



Part of the [Criminology and Criminal Justice Commons](#), and the [Information Security Commons](#)

---

### Recommended Citation

Tracy, Matthew Timothy, "Identity theft: A problem of complex systems or moral panic?" (2012). *Theses Digitization Project*. 4111.

<https://scholarworks.lib.csusb.edu/etd-project/4111>

This Thesis is brought to you for free and open access by the John M. Pfau Library at CSUSB ScholarWorks. It has been accepted for inclusion in Theses Digitization Project by an authorized administrator of CSUSB ScholarWorks. For more information, please contact [scholarworks@csusb.edu](mailto:scholarworks@csusb.edu).

IDENTITY THEFT; A PROBLEM OF COMPLEX SYSTEMS  
OR MORAL PANIC?

---

A Thesis  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---

In Partial Fulfillment  
of the Requirements for the Degree  
Master of Arts  
in  
Criminal Justice

---

by  
Matthew Timothy Tracy  
June 2012

IDENTITY THEFT; A PROBLEM OF COMPLEX SYSTEMS  
OR MORAL PANIC?

---

A Thesis  
Presented to the  
Faculty of  
California State University,  
San Bernardino

---


by  
Matthew Timothy Tracy

June 2012

Approved by:

  
Gisela Bichler, Chair, Criminal Justice

06-06-12  
Date

  
Deborah A. Parsons

  
Pamela Schram

## ABSTRACT

Identity theft can take on many forms including the theft of bank account numbers, photo ID's, driver's licenses, social security numbers, or credit card numbers. Today identity theft and fraud are on the rise. This problem deserves more attention and research than it is currently receiving. Some people view identity theft as an unstoppable crime.

This research aims to bring about a better understanding of the problem of identity theft. Moral panic perspective and complex systems perspective are applied to identity theft. Hypotheses are tested about the: prevalence of malicious outside hackers, vulnerability of different organization types to this crime, sophistication of identity breaches, lack of law enforcement response, and use of stolen personal records in further criminal activity.

The data were drawn from resources made available by a nonprofit organization called the Identity Theft Resource Center (ITRC). This is a cross-sectional study using secondary data supplemented by content analysis of news reports, and press releases. This study found most breaches to be employees using low-tech means. Consequently, if

organizations tightened up security measures in regards to their employees, identity theft and fraud could be largely preventable.

## ACKNOWLEDGEMENTS

First I would like to acknowledge Keith Castillo at the CSUSB computer lab for single handedly saving me on the formatting at a moment's notice. I would like to thank my family and grandma for all the support along the way. I want to thank Uncle Tim and Aunt Jan for all the support and encouragement to do well in school. I owe a special thanks to Blanca at the CSUSB rock wall for relieving my stress every day and showing me how to climb dangerously just the way I like it. I would like to acknowledge Morgan Smith for keeping my life interesting and for unknowingly motivating me to do well in everything I do. I am always in debt to Rachel Brandt for keeping my mind on what's important and for so many other things as well. I would like to acknowledge Dr. Schram, Dr. Parsons, and all the other Criminal Justice professors at CSUSB for everything they have done for me both as an undergrad and in grad school.

I owe everything to my chair Dr. Bichler, without her I would just be some dude who took a few grad classes once upon a time. Only with her guidance throughout every step in the process of writing this thesis and never-ending flow of knowledge was I able to achieve a Master's degree.

Regardless of what I choose to do or where I choose to go from here I feel like I can complete any academic program in the world if I wish too. The skills and knowledge I have gained during my stay at CSUSB have truly changed me and prepared me for anything. I owe a large part of that to Dr. Bichler, thank you for everything.

## TABLE OF CONTENTS

ABSTRACT .....	iii
ACKNOWLEDGEMENTS .....	v
LIST OF TABLES .....	x
CHAPTER ONE: INTRODUCTION TO IDENTIFICATION THEFT ....	1
CHAPTER TWO: A REVIEW OF THE LITERATURE .....	9
Cost .....	11
The Role of Police .....	12
Collection of Data .....	14
Exchanging Personal Information .....	15
Identity Theft Prevention on a Personal Level ....	19
Moral Panic Over Identity Theft .....	20
Hacker Profile .....	23
Complex Systems Perspective .....	27
Variables as Used in Past Studies .....	30
Variables of Interest .....	32
CHAPTER THREE: HYPOTHESES .....	41
CHAPTER FOUR: METHODOLOGY	
Data Source .....	44



Limitations of the Data Source .....	47
Underreporting .....	47
Generalizability and Reliability .....	48
Inter-Rater Reliability .....	49
Limitations of Data Set .....	50
Validity .....	51
Sample Description .....	52
Variables .....	54
CHAPTER FIVE: RESULTS	
Complex Systems Hypotheses .....	65
Moral Panic Hypotheses .....	69
CHAPTER SIX: DISCUSSION	
Complex Systems .....	80
Complex Systems Recommendations for Future Research .....	82
Complex Systems Policy Implications .....	83
Moral Panic .....	87
Moral Panic Recommendations for Future Research .....	92
Moral Panic Policy Implications .....	93

CHAPTER SEVEN: CONCLUSIONS .....	97
Final Statements .....	99
APPENDIX A: VARIABLES .....	101
REFERENCES .....	106

## LIST OF TABLES

Table 1. Concepts as seen in Past Literature .....	36
Table 2. Descriptive Variables .....	53
Table 3. Description of Complex Systems Measures .....	58
Table 4. Description of Moral Panic Measures .....	61
Table 5. Dependent Variable .....	64
Table 6. Hypothesis Test 1 .....	65
Table 7. Hypothesis Test 2 .....	67
Table 8. Hypothesis Test 3 .....	69
Table 9. Hypothesis Test 4 .....	71
Table 10. Hypothesis Test 5 .....	72
Table 11. Hypothesis Test 6 .....	73
Table 12. Hypothesis Test 7 .....	75
Table 13. Hypothesis Test 8 .....	76
Table 14. Hypothesis Test 9 .....	77

## CHAPTER ONE

### INTRODUCTION TO IDENTIFICATION THEFT

In November 2011 a computer server at Virginia Commonwealth University was hacked. The hacking was believed to be the work of someone with no affiliation to the University, and who resided within the United States. This breach exposed the dates of birth, social security numbers, electronic login information, and other aspects of the personal records of 176,567 people. In response the University hired an outside cyber security consultant to help contain the problem. The University is also advising those affected by the breach of how to get credit checks. It is believed that the hacker spent 16 minutes browsing through the server after hacking into it (Kapsidelis, 2011).

In a mere 16 minutes a hacker exposed the personal records of almost a quarter million people. Any one of these victims may at some point in the near or distant future become the victims of fraud that could have a far reaching impact on their lives. Identity theft is a crime that has the potential to affect everyone and it is on the rise. Yet it is much less understood than various other

types of crimes that are arguably less harmful. There is a gap in the literature about identity theft and a pressing need for this crime to be better understood in the hopes that it can one day be kept in check.

Identity theft assumes many forms including but not limited to the theft of social security numbers, driver's licenses or government issued ID cards, bank account numbers, birth certificates, check or credit card fraud, and computer fraud. In order for a crime to be considered identity theft enough information must be stolen in order to commit fraud. In other words, simply stealing an empty envelope with someone's name and address on it is not sufficient to be considered identity theft. If that envelope contained the person's new and current driver's license card and their social security number, then it would be considered identity theft. The purpose of this project is to test a theory of moral panic about identity theft, specifically to see if the characteristics of identity theft suggest it is an unstoppable crime, mainly committed by high-tech outsider hackers. A complex systems perspective that says online security systems are becoming more complex and interconnected will be tested too. In addition, current trends in identity theft are explored.

Instances of identity theft are on the rise, particularly with our increasing reliance on the internet (Erickson, & Howard, 2007). Today people all across the world fall victims to this crime and consequently their credit scores plunge, their life savings wither away, they get in deep debt, and in rare cases they even lose their homes, jobs, and their way of life as a result of falling victim to this crime. It is commonly believed that police have little influence on identity theft; sophisticated hackers live in other countries where police and even United States federal agents do not have authority to prosecute them. In some cases, their own governments fail to act out of apathy or lack of the resources to enforce any anti-identity theft rules. As demonstrated with the introductory case, a single breach can expose thousands of people. Those exposed could fall victims to fraud years after the incident.

These commonly held beliefs might be indicative of a developing world-wide moral panic over identity theft. A lot of people and even businesses do not understand this problem, know how to prevent it, or know what to do if they fall victim to fraud or identity theft. Since identity theft is a relatively new phenomenon there is no classic

literature on the subject. This problem is under-researched and deserves a lot more academic attention than it receives. It is vital that this crime becomes better understood so intelligent, sound policy implications can be formed and identity theft can be better kept in check.

The limited research available suggests findings that contradict widely held beliefs. Most identity theft breaches are not purely the result of high-tech outside hackers. Instead, most breaches are the result of an insider (from within an organization), lost or stolen credit cards and bank account information, administrative error, or accidental exposure of personal information. However, instances of identity theft and high-tech online or computer identity theft are on the rise. The year 2002 had more instances of online identity theft than in the previous ten years combined (Erickson, & Howard, 2007).

The business sector seems to be more vulnerable to identity theft and fraud than any other industry including medical, military, and education sectors. Also it appears that the majority of identities stolen are never used to commit fraud and that high-tech identity theft breaches affect people in larger areas than low-tech breaches (Identity Theft Resource Center, 2011).

Hypotheses derived from these observations can be tested by using a data set developed from source materials assembled by a non-profit organization called the Identity Theft Resource Center or ITRC. The ITRC keeps a data base of all known identity theft events from the year 2010 that have been covered by at least one reliable news source. The ITRC data base includes 662 breaches from the year 2010. Due to the amount of detail provided and the large sample size, this data set has a relatively strong generalizability making it the best national source for this research. This source includes all the necessary information to code the variables of interest.

The research design involves a correlational study using a data base built from ITRC information supplemented with content analysis of supporting documents. Contingency tables, Chi-square, and AVOVA, are used to test eleven hypotheses derived from the moral panic and complex systems perspectives. A possible limitation of the study is the underreporting of identity theft cases. The ITRC includes many confirmed identity cases from the year 2010; the ITRC certainly does not capture every case of identity theft in the United States that occurred during 2010. Businesses, especially financial institutions, have a strong interest



in not reporting breaches because it may make them look bad to customers. Therefore, underreporting is a persistent challenge for identity theft research.

A majority of breaches examined for this project were electronic and low-tech. More breaches were committed by employees than outside hackers. When victimized organizations responded to breaches they usually responded within a week of discovering the breach. Law enforcement did not respond to most breaches in any way except for taking a report of the incident. Most breaches included in the data set were covered by a news article or news source. Letters to the Attorney General's office was the next most common source of breach information.

With regards to the complex systems perspective there was a weak to moderate and highly significant relationship between hacker's skill level and notoriety. If a breach involved high-tech hacker skills it was more likely to affect people in a larger area than if the breach only required low-tech skills. With regards to the moral panic perspective there was a moderate to strong and highly significant relationship between hacker's skill level and locus of violation. If a breach was committed by an employee it was more likely to be low-tech; whereas, if it

was committed by an outside hacker it was more likely to be high-tech. If a breach was committed by an outside hacker with inside help it was about equally as likely to be a low-tech or high-tech breach. There was a weak to moderate relationship between records exposed by breach type and nature of breach. Breaches committed by outside hackers were predominately electronic. Breaches resulting from administrative error were about half electronic and half paper. Breaches resulting from employees were mostly electronic as well.

There appears to be a bimodal pattern to identity theft where a large volume of cases are high-tech outside hackers or low-tech employees. The middle ground seems to be disappearing. Future research should look at hacker groups to see if they are becoming more specialized. If they are this could be more evidence for the complex systems perspective. Since breaches resulting from employees are still the most common type of breach businesses and organizations should tighten up employee security and implement new training measures. Organizations could make employees log onto computers using a unique password so their activity could be tracked better. Only

granting access to sensitive information for employees who need it to do their jobs will also be beneficial.

Law enforcement infrequently responds to identity theft cases. It is unclear whether this problem is due to a lack of resources or if such cases receive a low priority until subsequent, related frauds are discovered. In any event, increasing law enforcement reactivity is crucial. Since a majority of identity theft cases are low-tech law enforcement will be able to significantly reduce this crime with conventional target hardening initiatives; high-tech solutions are not necessary.

## CHAPTER TWO

### A REVIEW OF THE LITERATURE

Identification theft assumes many forms such as stealing and using someone else's credit card, social security cards, electronic bank accounts, and forging signatures on checks. Identification theft or ID theft is a crime that has become an increasing problem with the electronic age. The increasing global reliance on electronic means to verify people's identity and to transfer money leads to greater and more costly incidents of identity theft.

Identity theft is often considered a high-tech crime. This crime can be hard to trace especially for law enforcement because many agencies do not have sufficient resources dedicated to identity theft. Identification theft is a crime that affects individuals and corporations alike. If businesses do not secure client information, then corporate reputations suffer, business can be lost, and subsequent lawsuits might fatally impair the organization. There are also repercussions for the individual who had their identity stolen; a thief can take the person's entire life savings, leaving a person who was previously in good

financial standing in debt. In addition, our criminal justice system is not particularly hard on identity thieves who just steal information in comparison to those people who commit street crimes, although they steal a lot more than street criminals typically do.

With an increasingly complex and technologically advanced society, we rely on our computers and advanced electronics more and more for almost every aspect of life, from social networking to banking, and this means more opportunities for identity theft and eventually fraud. Regardless of what precautionary steps are taken to prevent fraud and identity theft, everyone is still at risk. There is no full proof method to successfully guard against identity theft and fraud one hundred percent of the time, but some methods do work better than others (Identity Theft Resource Center, 2010). The cost of fighting identity theft and fraud, the role of police, and the problems associated with identity theft are all discussed next. Also a possible moral panic over identity theft and complex systems are reviewed briefly. Finally, findings and variables from the past literature are discussed.

## Cost

Estimates suggest that identification theft in the United States annually costs \$50 billion, and the total annual cost of identification theft to individuals whose information is stolen is about \$5 billion a year (Federal Trade Commission, 2009). Identity theft could lead to higher prices for goods and put small companies out of business because of the staggering amount of money it costs some of them to deal with this crime.

There are also some less obvious costs associated with identity theft such as time spent. Time spent can be on a personal level, which is where victims of identity theft have to clear their names, which means making a lot of phone calls, driving to places, and seeking the help of others. This could lead to less time spent with family or at work. Among business victims there are also hidden costs, such as the time of business executives who have to clear their companies' name. Sometimes this cost is so high that companies even have to hire their own identity theft personnel. Also different branches and departments within the United States government hire specialized personnel to deal with identity theft for that department. So identity

theft even costs taxpayers money. This means that in a way everyone who pays taxes is a victim of identity theft.

### The Role of Police

Identity theft became a federal crime in 1998. However, police do not often do very much to prevent this crime. In addition most police agencies do not have special units designated to identity theft or fraud because they simply do not have the resources available to do so, and even if they did officers would probably spend countless hours for every bust. This is likely because identity theft is often more complicated, harder to trace, and less visible than most other crimes police departments deal with (Newman, The problem of identity theft, 2004). Often police agencies cannot differentiate between identity theft victims that come to them because they are inconvenienced and those that are suffering. It has been suggested that police often do not respond within a timely manner and they may even take weeks before looking into a breach; law enforcement agencies are ill equipped to deal with fraud and identity theft (Newman & McNally, Identity theft literature review, 2005).

Few police agencies maintain a dedicated cyber unit, where officers (or other sworn personnel) browse the Internet for illegal activity. This takes money and resources. Police can keep records of reported identity theft incidents as well, but in reality the role that police currently play in the prevention of identity theft is quite limited. Further it is difficult to prosecute this crime because often little evidence is left at the "scene" of the crime. It is up to the victim of identity theft to find out he/she has been victimized and then to inform the police and the Federal Trade Commission or (FTC) within a timely manner so an investigation can begin (Federal Trade Commission, 2003). Police are equipped to do little more than take a police report.

Some evidence suggests that businesses are becoming the victims of identity theft more often. Identity thieves are using business names, addresses, and other information to apply for loans or impersonate sales staff to sell products to customers, and obtaining their credit card numbers. This type of identity theft is yielding greater profits for identity thieves because business bank accounts usually have more money in them than private ones, and businesses also qualify for a range of much larger loans.



For example, nearly 70% of identity theft cases are committed in the workplace or by people claiming to be employees (Collins, 2003). It would be useful to know if attacks are still primarily being made by inside employees or if outside hackers are on the rise. This also hints that a fear over an increased prevalence of high-tech outside hackers might be a myth, or at least it appeared that way in the year 2003.

#### Collection of Data

Personal information can be collected in several legitimate ways: for example, people can fill out a credit card application, fill out a job application with their social security number, they can provide personal information to their tax consultant, and people tend to provide some personal information to cell phone companies when getting a new plan. Also life insurance agents carry personal information on their laptops (Prosch, 2009).

Illegitimate methods of obtaining personnel data also exist. For instance, thieves can dig in trash cans for papers containing personnel information that have not been adequately shredded or employees who work in companies who collect personnel data may also steal it. Identification

thieves can send out illegitimate emails asking for personnel information and hack into or physically steal computers containing this kind of information.

### Exchanging Personal Information

Another problem with identity theft is that often businesses must exchange client information with other businesses, tax lawyers, and government offices (Newman, Check and card fraud, 2003). When personal information undergoes third party transfers there is an opportunity for it to be misplaced, stolen, or viewed by additional parties that do not need to be exposed to this confidential information. Sometimes third parties receiving the information may themselves sell or give the information to other sources who in turn might commit identity theft.

Check fraud is another way that people commonly steal the identity of others. This is a unique type of fraud because banks usually try to hold the merchants who accepted the checks, or the victim responsible for these losses. The banks and the merchants who accepted these fraudulent checks often fight over who has to cover the losses. These disturbances can lead to more check fraud (Newman, Check and card fraud, 2003). Merchants typically

do not want to get police involved in these types of situations and they would prefer to handle it on their own because they might think that getting the police involved could scare off customers or give the company a bad reputation. It is commonly assumed that law enforcement does not possess the tools to adequately deal with identity theft. In addition, businesses might think that the cost of doing something exceeds the cost of doing nothing about the problem (Newman, Check and card fraud, 2003).

The lack of cooperation between agencies and lack of effective criminal justice sanctions encourages thieves to continue practicing fraud. Newman (2003) has shown that only about one in four fraud incidents ever get reported to police. In addition, the same study found that 80% of the public thinks it is easy to commit credit card fraud (Newman, Check and card fraud, 2003).

In the electronic age people can commit check fraud on a computer without ever showing an ID. In fact one study found that this type of check fraud accounted for 23% of all fraud, and lost or stolen cards accounted for 28% of all frauds. Mail that gets stolen accounted for 6% of all fraud, and the leading type of fraud was counterfeiting which accounts for 39% of all fraud (Newman, Check and card

fraud, 2003). Counterfeiting usually means that a professional is behind it because this type of fraud requires the making of fake documents, which often takes a descent amount of resources to do. This could be evidence of two myths plaguing our society. One is that high-tech outside offenders could be on the rise and committing identity theft and fraud more and more often. The second myth that is suggested here is that identity theft may be an unstoppable crime and the evidence for this would be that only one in four incidents of identity theft are ever reported to police. So three fourths of the time victims might assume that the crime is unstoppable and unsolvable so they do not even bother reporting it.

With today's global market, people from other countries can commit identity theft too. This poses additional challenges for detection, investigation and prosecution. While many nations have laws against it many face the same enforcement challenges, i.e. do not possess the means to enforce laws. However, all identity thieves use the same methods so a sound prevention strategy should work for both (Waldman, 2006).

Wadman (2006) found that some companies are increasing the level of scrutiny and investigation into some papers

and documents that are of potentially high value to identity thieves and this tactic alone has been demonstrated to have some success. The same study also demonstrates that some cutting edge technology out there, which through the use of complex formulas screens some documents and decides which one's should be chosen for additional screening. This is based on how likely the document is to fall victim to identity theft or be a fraudulent document already (Waldman, 2006). This strategy involves risk assessment and selective target hardening.

Another problem with identity theft is that personal information often expires for businesses. When this happens it is no longer useful to businesses, and sometimes it is not destroyed immediately after this happens. This same information does not expire to identity thieves and it can still be used to commit fraud after it becomes useless to businesses (Prosch, 2009).

Collins (2003) found that 70% of all identity thefts committed in the workplace are committed either by employees or by people impersonating employees of a particular business. These thefts were committed in person meaning that they are not done solely online from a person who has never physically been to the business. Cyber

hackers account for less than a third of all business identity thefts. In addition, according to this study identity theft tends to be linked to drug trafficking and not surprisingly organized crime (Collins, 2003). This trend could be changing though and cyber hackers could be becoming more prevalent.

#### Identity Theft Prevention on a Personal Level

Businesses seem to be a big part of the problem with identity theft because they are the ones asking people for their identities. Individuals can also contribute and make themselves more vulnerable to identity theft as well though. For example people can be careless with personal items such as bringing personal laptops into work or leaving credit cards, social security cards, driver's licenses, or other personal information visible in public places.

Another major problem with identity theft is that a lot of people do not take it seriously until it happens to them. Regardless of how careful one is with their identities everyone is always at some risk of identity theft. People sometimes do not use antivirus software on their computers and frequently send personal information

out in emails or post it in online chat rooms (Federal Trade Commission, 2003).

### Moral Panic Over Identity Theft

The media may be contributing to the development of a moral panic over identity theft by playing on the social fear this crime creates when it perhaps should not. Content analysis of 257 newspaper articles from 1995 to 2005 found clear evidence of repeated statements that it was easy to commit identity theft through electronic means (Morris & Longmire, 2008). Further, a growing percent of the media reports suggest that identity theft is unstoppable; in 2008, 15% of newspaper articles on identity theft claimed that the problem was unstoppable (Morris & Longmire, 2008).

The media called 17% of sophisticated identity theft crimes unstoppable and 33% of highly sophisticated identity theft crimes unstoppable. Thus, a large proportion of reports suggest that highly sophisticated instances of identity theft are unstoppable. This in turn is suggestive of an epidemic (Morris & Longmire, 2008). This could be due in part to the media's lack of understanding of identity theft.

Wall (2011) suggests that cybercrime is constantly evolving in order to evade law enforcement and prevent being caught. Furthermore cybercriminals evade attempts to control them by using different means to commit crimes as soon as law enforcement can catch onto their techniques (Wall, 2011).

Gogolin and Jones (2010) found that 42% of law enforcement agencies do not even have a computer crimes unit and 34% of agencies had acquired one within the last four years. The study found that only 40% of new police officers in training in the United States received any type of training regarding electronic crimes and there was no training of the sort available for existing officers. In addition 73% of electronic identity theft investigators nationwide receive five or less days of training on the subject annually. Agencies have less than 4 primary investigators for electronic identity theft and most were also responsible for other types of cases (Gogolin & Jones, 2010).

Furthermore only 90.50% of law enforcement agencies nationwide have ever investigated an identity theft case. The study concluded that law enforcement is certainly behind when it comes to dealing with digital or electronic



crime of all types (Gogolin & Jones, 2010). Judging by these findings one would expect to see that in the majority of electronic identity theft cases law enforcement would not respond in any way beyond taking a report. If true this finding would suggest that even law enforcement is ill equipped to handle this crime and they too might find systems to be getting ever more complex, interconnected and harder to deal with.

Cyber gangs never meet in person and are loosely organized with no clear leadership (Wall, 2011). These gangs tend to specialize in one area such as credit card fraud, bank fraud, phishing, or stealing social security numbers (Hetu, Chit-Hack information exchange paths in IRC hacking chatrooms, 2011). Cyber gangs are located worldwide with an increasing number of them coming out of the Middle East and India (Wall, 2011). One cyber gang for example specialized in Warez (or pirated software) and they would crack security codes in new software and then release them to the public. This gang called themselves "Drink or Die." There is even a gang that specializes in auction fraud on eBay. This goes to show that these gangs have unique specialties and do not tend to commit every type of cybercrime there is. There are three major types of

cybercrime; crimes against the machine such as hacking, crimes in the machine such as hate speech, and crimes using the machine such as fraud. Cyber gangs do not tend to commit crimes in more than one of these categories. These gangs often get inside information from an employee of an organization who makes the software (Wall, 2011).

Even though, computer trespassing already has relatively harsh punishments in the United States compared to crimes that cause physical harm to others. Erickson and Howard (2007) argue that these harsh laws and penalties do not seem to have the deterrent effect desired because such crimes are on the rise. This study analyzed 550 cases reported in printed news sources. Erickson and Howard (2007) found that there were three times as many identity theft incidents in the year of 2005 as there were in the past 25 years before that combined (Erickson & Howard, 2007). This suggests that identity theft is sharply on the rise.

#### Hacker Profile

One study found that some of the largest groups of computer hackers in the United States are not motivated by money. Often their level of success in the hacking world is determined by the response they get from their peers. These

hackers hack to be recognized by their peers and are not in it for the money. There is no shortage of consumers who are attracted to their services either. The study identifies two distinct categories of hackers, hacking groups and amateurs. Members of hacking groups often spend 40 plus hours a week illegally obtaining and redistributing materials without any legal copyright to the materials (Hetu, Morselli, & Langlois, Welcome to the scene: A study of social organization and recognition among Warez Hackers, 2011).

Amateurs just download one illegal song or movie to a peer-to-peer network once in a while. Hacker groups have become international in recent years and whenever a member or even a small subgroup of people within a larger hacker group releases some pirated information other members in the group see it as a challenge to release pirated information of their own that is worth more. These hackers are motivated by the shared belief that information should be free, pride, and the need to belong to a group. These groups of hackers are also self-organized and there is no clear leader but rather just a lot of members each with their own status which depends on their hacking successes. The findings in this study indicate that on average each

hacker group is in contact with 6 other groups that compete with each other. These groups generally do not last long, they offer products of low value and they tend to only specialize in one type of piracy like movies or songs for example. This study examined an online index composed of data on illegal content that was publically available from 2003 to 2009 (Hetu, Morselli, & Langlois, Welcome to the scene: A study of social organization and recognition among Warez Hackers, 2011).

Hackers often talk to each other about hacking online through the use of chat rooms such as MySpace or Facebook. However hackers seem to prefer one chat room in particular and that chat room is called IRC. IRC is an online network where people can post messages that are then viewable by the public. Unlike most other chat rooms over two thirds of the people who participate in this chat room talk about hacking. Over 90% of the talking is advertising hacker services or generic repeated messages that are done by bots created by hackers. There are hacking groups and people who talk with one group, they rarely talk with anyone else in the chat room that is outside that particular group. The median number of members in one of these groups is seven with one person who appears to be at the center of the

network. Other members often talk to each other through messages to the person who is at the center of the network. The members in these groups appear to be close and to know each other (Hetu, Chit-Hack information exchange paths in IRC hacking chatrooms, 2011).

There has also been a recent evolution in scareware which is a popup that tells people they need to purchase particular antivirus software immediately or their system will be destroyed. Often if this protection is purchased it will be dormant for a while (so it becomes harder to track) then it will weaken a computer's defenses against viruses. Scareware usually involves a small amount of money from one person but one scam can be worldwide which adds up to a good sum of money. These scams are relatively simple technologically speaking and often go unreported because when people get stiffed for \$25 it is not common to go to the police who often times know nothing about the problem anyway (Wall, 2011). Again cybercrimes cannot be stopped, they can only be managed. This fact coupled with a lack of understanding about identity theft in general might be leading to a moral panic over what is perceived as unstoppable identity theft and cybercrime.

## Complex Systems Perspective

Complex Systems perspective says that today online systems of all sorts are getting ever more complex. This goes for all sorts of online systems from security, to online chat rooms, to the news, and to the way information is shared and kept secret online all together. Complex systems perspective says since everything is getting evermore complex and valuable, hackers can cause bigger and bigger problems when they succeed in hacking an online system. Also since these systems are interconnected it is possible for a hacker to gain access to all of them. As systems are becoming more and more complex, breaches from outside hackers may be more high-tech. Most identity theft cases still involve a problem or issue within a company though, such as an employee committing the offense or administrators accidentally leaving a computer screen turned on with a page of customers' credit card numbers open. These types of breaches are still low-tech crimes (Zhu, Security control in inter-bank fund transfer, 2002).

Security systems today are large, complex, and interconnected, which makes hacking difficult. System breaches might be becoming more like earthquakes, whereas in the past when security systems were less complex and

interconnected breaches were more like rainstorms. Breaches might be increasingly rare and devastating when they do occur (Zhu, Security control in inter-bank fund transfer, 2002). If this is true then one would expect to see a lot of breaches that are large in scope, and expose the personal records of a large number of people. This in turn also adds to the evidence of a moral panic theory over identity theft. If complex systems theory is correct then instances of complex electronic identity theft and fraud should be plentiful while instances of low-tech identity theft should be increasingly rare.

In addition if the online cyber world is getting evermore complex and harder to understand and there is a moral panic over identity theft attacks coming from this cyber world then one would expect to see more and more law enforcement agencies specializing in this area. If online identity theft is becoming more and more high-tech, law enforcement might be less likely to respond to an identity theft crime in any way other than taking a report. In other words law enforcement may not have the resources to launch a detailed investigation or follow a complex electronic trail.

In the high tech world of the 21<sup>st</sup> century once an identity thief has someone's personal identity creating a fraudulent credit card or check is very easy to do (Katherine, Jackie, & Paul, 2008). In other words once personal information is exposed technology is readily available to commit fraud. For example credit cards can be used on the internet without the use of an ID to go with them. In the future technologies that guard against identity theft might get more and more complicated and difficult for laymen to comprehend. Therefore people in the general population will be able to protect themselves less and less because they will understand the technology used to prevent identity theft less and less.

An increased complexity in online systems could mean that fewer and fewer online identity theft attacks are successful, but when an attack is successful the amount and value of information exposed is larger because more complex systems could be connected to or integrated with one another. So once a breach is successful in one system it can be successful in many. If this was true one would expect the data to show that as systems become more and more complex the number of successful hacking incidents decreases, but the number of personal records with each



successful breach increases. In other words when a successful breach does occur it should be more damaging.

Groups tend to specialize on a specific kind of hacking, like hacking into one type of system such as Microsoft XP or Norton antivirus software for example (Hetu, Chit-Hack information exchange paths in IRC hacking chatrooms, 2011). Hackers generally have close ties to other members of their group, they usually have small groups that specialize in one type of hacking and there appears to be no evidence of a rise of the malicious hacker. However there does seem to be a good number of sophisticated hacker groups but there is not a whole lot of evidence to suggest that they are more malicious than in the past.

#### Variables as Used in Past Studies

Victimization levels vary by sector. The Erickson and Howard study grouped reported incidents of identity theft by sector and found that the commercial sector was responsible for the most incidents of identity theft, followed by the educational sector, then the government sector, then the medical sector, and lastly the military sector (Erickson & Howard, 2007). The commercial sector was

responsible for the most people's personal information exposed, with over three times as many records exposed as the next sector which was the education sector. The medical sector had over 7 times as many incidents of identity theft as the military, the number of personal records exposed was nearly the same with 4.6 million records exposed whereas the military had 4.3 million records exposed (Erickson & Howard, 2007).

The data also showed some incidents where records or personal information was exposed but no records were actually compromised or used. Reported incidents and volumes of compromised records were also sorted out by the type of breach. Interestingly missing or stolen hardware accounted for the majority of incidents at 199 out of 550 incidents, followed by incidents of being hacked from the outside which accounted for 172 incidents. Next were people exposing themselves online at home or on their own, this accounted for 84 incidents. Next were unspecified breaches with 51, then insider abuse with 26 incidents, and lastly incidents resulting from administrative error. There were 18 incidents in the last category. However hacked information accounted for the second most records exposed, surpassed only by the number of records exposed by

unspecified breaches. The next most records exposed came from the category missing or stolen hardware followed by the category administrative error (Erickson & Howard, 2007).

The Erickson and Howard study (2007) examined hacker and organizational culpability in reported incidents of compromised records. Only 31% of hacking incidents were attributed to a hacker, whereas 60% of incidents were attributed to insider abuse or theft, or administrative error, or accidentally exposing information online. The other 9% was unattributed or unspecified. The study concluded that only 40% of incident reports involving hacking involved malicious hackers that had criminal intent (Erickson & Howard, 2007).

#### Variables of Interest

In the information age people view the coming of technology and global online communications in two ways, one as a technology of progress that can change the lives of many for the better, and two as a technology that can undermine traditional institutions and destroy people. This second view on technology is what might be leading to a moral panic over new and complex online systems and technologies. Cyberphobia and cyberfear have contributed to

a moral panic over online identity theft and fear of the internet in general. This moral panic is generated by threats to public life such as cyberwarefare, threats to private life such as online stalking, threats to personal culture such as hacking and a loss of privacy, and threats to collective culture such as the destruction of copyrighted media (Sandywell, 2006). The author in this study argues that the public distrust of technology is leading to a moral panic.

Several variables can be used to test this theory of moral panic. First the locus of violation must be taken into consideration. In other words was an outside hacker or an inside employee responsible for the identity theft. Another variable that is crucial to testing a moral panic over online identity theft is the method that was used to commit the identity theft. For example this could be the theft of a hard copy of an employee social security number and other personnel information or a high-tech online scam, in addition rather the personnel information stolen was ever criminally used is also important. If there is a moral panic over identity theft then most or at least a good portion of information stolen or exposed as a result of identity theft should be used to commit fraud or criminally

used in some way. Another important variable is the response of the business or organization once they found out there was a breach. This variable is important because if organizations are not taking identity theft seriously and a lot of people's identities are being used to commit fraud then it may not be high-tech crimes. It could just be teenagers who are not being caught or prosecuted. Also the time elapsed from the breach to the response of the organization is important for the same reason.

Notoriety is an important variable for testing the complex systems perspective. Notoriety is the scope of a breach or if the theft is only local, regional or if it's national or maybe even international. This is important because in theory the more high-tech the crime the farther reaching it should be. In other words if all identity theft crimes are ultrahigh-tech then it is also quite possible that they target international targets because it would be harder to catch and prosecute the hackers responsible. Also if systems are becoming more and more complex one would expect to see this trend.

According to the Federal Trade Commission in 2009 the west, southwest, southeast, a select few states in the far northeast, and Illinois had the most complaints of identity

theft per 100,000 people. The Federal Trade Commission used self-report surveys to get their data (Federal Trade Commission, 2009). This finding is important to the study at hand because the northeast has a greater concentration of states that have a mandatory reporting policy for identity theft than any other part of the country, so it should be a little overrepresented in any sample. It is not overwhelmingly the most common source of identity theft in 2009 according to the Federal Trade Commission so it should not represent too high of a percentage of the sample of identity theft cases in 2010 either. Below in Table 1 is a list of the main concepts and their descriptions as defined in past studies.

Table 1. Concepts as seen in Past Literature

Concept	Assumptions Examined	Existing Evidence	Research Question
Moral panic			
Breach type	External attacks are currently most prevalent.	The majority of identity thefts were due to an inside employee, administrative error, or missing or stolen hardware. The number of unspecified breaches was also large. (Erickson & Howard, 2007)	How many incidents of identity theft were due to an outside hacker, an inside employee, missing or stolen hardware, people exposing themselves, administrative error, or unspecified breaches.
Use of information	The information stolen is used for criminal purposes.	Rarely is information used to further other criminal activity (Erickson & Howard, 2007) (Sandywell, 2006)	Was any of the information stolen ever criminally used (or if fraud was ever committed)?

Concept	Assumptions Examined	Existing Evidence	Research Question
Response of organization after victimization	Breaches are not consistently reported to the public/victims.	Organizations usually alert people whose identity may have been stolen (Morris & Longmire, 2008) (Wall, 2011).	Did the organization respond accordingly to the victimization and alert people of possible security breaches involving their personnel information?
Time elapsed from victimization to organization's response	When breaches are reported at all it is usually in a timely fashion.	It usually takes organizations a few days to notify all those who might be affected (Morris & Longmire, 2008) (Wall, 2011).	Did the organization notify people and take appropriate action in a timely manner after learning of a breach?



Concept	Assumptions Examined	Existing Evidence	Research Question
Victim sector	Victimization is uneven; the following sectors are organized from greatest to least victimization frequency: business, education, military/government, medical organization.	Businesses are victimized disproportionately more than all other sectors (Erickson & Howard, 2007).	Which sector is victimized the most second most and so on; business, education, military, government, and medical?
Offender Type	Administrative errors accounted for the most exposed records, missing or stolen hardware and outside hacker also accounted for high numbers of records stolen.	Administrative error, employees, and hackers account for nearly all identity theft incidents (Erickson & Howard, 2007)	The number of records exposed for each of the following breach types: outside hacker, an inside employee, missing or stolen hardware, people exposing themselves, administrative error, and unspecified breaches.
Complex systems			

Concept	Assumptions Examined	Existing Evidence	Research Question
Locus of violation	Attacks are most likely to be initiated by an employee or outsiders with connections to employees.	(Erickson & Howard, 2007) (Federal Trade Commission, 2000) (Sandywell, 2006)	Who committed the offense, was it an advanced hacker from outside the organization, or was it an employee from the inside?
Method of attack	Most attacks involve low-tech methods where hard copy of personnel information or administrative error.	(Sandywell, 2006) (Zhu, Security control in inter-bank fund transfer, 2002)	Was the attack done through an online security breach or was a hard copy of personnel information stolen (low-tech method)?
Notoriety	Most attackers target local organizations.	(Sandywell, 2006)	Was the attack local, regional, national, or international?
Incident Characteristics			

Concept	Assumptions Examined	Existing Evidence	Research Question
Region	No one region in the United States is responsible for an overwhelming majority of breaches. The northeast is the region with the most breaches.	(Federal Trade Commission, 2009)	What region in the United States is responsible for the most identity theft breaches?
Dependent Variables			
Exposure	The number of personal records exposed varies significantly depending on other variables.	(Erickson & Howard, 2007)	How many people's records were exposed in the business sector, government, educational, military, and the health sector?
Skill Level	The majority of identity theft breaches are low-tech but an increasing amount are becoming high-tech.	(Zhu, Security control in inter-bank fund transfer, 2002)	Are identity theft breaches predominately high-tech or low-tech?

## CHAPTER THREE

### HYPOTHESES

Nine hypotheses are used to test the moral panic and complex systems perspectives. Hypotheses one and two deal with complex systems and hypotheses three through nine are for moral panic.

Hypothesis 1: High-tech identity theft incidents are more likely to be large in scope and affect people nationally or internationally, whereas low-tech identity theft incidents should generally be smaller in scope and only affect people who reside locally or regionally.

Hypothesis 2: Inside employees and outside hackers with inside help are responsible for more low-tech identity theft incidents while outside hackers are responsible for more high-tech incidents.

Hypothesis 3: Electronic security breaches are more likely to involve high-tech hacker skills than low-tech hacking.

Hypothesis 4: Law enforcement is more likely to respond to an identity theft incident if a business is victimized than if it's an educational institution, medical

institution, or military/government agency that is victimized.

Hypothesis 5: The business/financial sector is also responsible for the most records exposed followed by education, government/military, and the medical sector is responsible for the least records exposed.

Hypothesis 6: Internal breaches (administrative error, employee theft, and missing or stolen data) are more likely to involve paper identity theft incidents, whereas external hackers are more apt to commit electronic attacks.

Hypothesis 7: Outside hackers expose fewer personal records than other types of attackers (e.g. employee theft, administrative error, or missing or stolen data).

Hypothesis 8: The majority of personal records exposed in identity theft incidents are not criminally used.

The literature on identity theft suggests that all organizations are equally likely to respond to information security breaches in a reasonable time. For example if an organization is victimized and they respond by notifying law enforcement and if another organization is victimized and they respond by notifying those affected, in theory they will both respond in about the same time, even though notifying law enforcement is easier and should be quicker

than sending out notices to what can sometimes be thousands of people. A reasonable time is assumed to be one week between the date the breach is identified and the date that the primary news source is published (with reliable information about the incident).

Hypothesis 9: No difference is expected among organization response types in the timeliness of public notification.

## CHAPTER FOUR

### METHODOLOGY

The research design involves a correlational study using secondary data that was supplemented with content analysis of supporting documents. The information used was drawn from the Identity Theft Resource Center or (ITRC). Several variables were taken directly from the 2010 ITRC breach report and others were coded from supporting documents linked to each case. This chapter describes in detail the data source, its limitations, and the data set. Generalizability, reliability, and validity, are also addressed. Variables are then discussed, and the chapter concludes with an evaluation of the resulting data set.

#### Data Source

This study draws information from a public warehouse made by the Identity Theft Resource Center (ITRC). This source includes 662 incidents of identity theft from the year 2010. Most incidents listed include links to supporting documents such as the news article that discussed the case. At the time of this project one link was not functioning leaving 661 cases with supporting

documents. The ITRC only includes a breach in the data set if supporting documents are deemed to be credible or if they can back it up with another news source classified as credible (Identity Theft Resource Center, 2011). The ITRC did not use a sampling method at all: instead they simply included every identity theft event from the year 2010 that was covered by a credible source in the United States. This is not to say that every identity theft incident that occurred in 2010 is included in the data set. The ITRC stated that they are certain that their data set is under representative of the identity theft problem but do not estimate the volume of missing cases (Identity Theft Resource Center, 2011).

This study extracted information about security breaches that are published online in a document titled "Breach Reports 2010". The ITRC defines a breach as any event where a person's social security number and any other information needed to commit some kind of identity theft is exposed. The ITRC follows US Federal guidelines as to what specific information compromises an individuals' identity. A drivers' license, credit card or bank number, medical record, or financial record coupled with a social security number is considered enough private information for



identity theft. Breaches may be paper or electronic and stolen identities do not need to be used criminally in order to qualify as identity theft.

It should be noted that the theft of encrypted data does not count as identity theft unless the thief also has in their possession, the coding required to read the information. This is because the theft of encrypted data is not an identity theft threat because the information cannot be read, and it is rare that a thief also has in their possession the coding needed to read that type of information. Items such as laptops, that are stolen and that contain personnel information but are protected with a password were classified as identity theft. This is because a password is not considered adequate protection against identity theft (Identity Theft Resource Center, 2011).

ITRC's listing of cases is one of the most comprehensive and publicly available set of events. The ITRC is a federally funded non-profit entity mandated to keep track of all known breaches; eight full-time employees work for the ITRC and they comb through all available news sources to identify relevant cases. Since each case included contains links to all original information sources, this compilation process is invaluable to the

current study. Accessing these original sources enables the development of variables and coding strategies to directly test a wide range of hypotheses. Proxy variables are not necessary.

#### Limitations of the Data Source

Since ITRC does not provide an exhaustive list of news sources used to identify potential information security breaches it is not possible to ensure that only credible news sources are used. This likely resulted in some underreporting. In addition, the ITRC's main focus is identity theft breaches that are based in the United States and thus, even if a breach was covered by credible news sources outside the United States it would probably not have been included into the data set unless it was also covered by a credible news source within the United States, in which case it would be in ITRC's database.

#### Underreporting

Underreporting is possible for certain types of incidents. Not all major breaches are reported to news agencies. This is a general problem associated with identity theft research as there is a vested interest on the part of business and government agencies to keep the victimization private. Moreover, victimization affecting

individuals is not likely to draw public attention. Further a handful of states do not mandate the reporting of identity theft incidents, mandate disclosure policies typically apply to individuals and entities located within the state. Only 29% of the breaches in the sample came from states with mandatory reporting laws (Identity Theft Resource Center, 2011). Since a majority of cases did not come from states with mandatory reporting laws, this means they are not overrepresented in the sample which is good for external generalizability.

#### Generalizability and Reliability

Secondary analysis has strong generalizability due to the breadth inclusiveness of the cases examined. As noted previously, the ITRC is a well-funded organization employing 8 researchers. This group is able to generate a more complete sample than what a single researcher on their own would be able to create in a reasonable time (Bachman & Paternoster, 2004). The inclusive case identification process used leads to the formation of a comprehensive data set of all the confirmed identity theft incidents in 2010 that were covered by credible news sources in the United States. In total, 662 cases constitute a large sample size

for identity theft incidents so generalizability should be "strong" (Identity Theft Resource Center, 2011). ITRC's data set is one of the most comprehensive and detailed data sets on identity theft around today.

Every researcher wants their research to be reliable so that their findings can be reproduced and confirmed throughout the scientific community. When the data set was created using content analysis, all coding was done by a single researcher who double checked his work. After recoding ten cases the reliability of this researcher's coding is estimated at 93.66% reliable.

#### Inter-Rater Reliability

In order to check the data set for reliability ten random cases were recoded after the data set was complete. These cases were then in turn cross checked with the way they were coded the original time. This checked for researcher error in the data set. The ten studies that were cross checked matched up 93.66% with their original coding. So it can be assumed that the coding is 93.66% reliable for this project.

## Limitations of Data Set

First it should be noted that the data set assumes all limitations of the data source. Due to the ITRC's selection criteria the number of international cases is vastly underrepresented in the data source and by extension also in the data set used for this project. In addition after having read all the news articles it appears that sometimes when a victim or company is unsure who committed an attack they will often point to an outside hacker, as this might make them look better than if it was an employee and they could not trace it back. Also when police were unsure of who committed a burglary they often said it was an outside hacker. Out of 661 total cases 39 were burglaries. So outside hackers might be slightly overestimated in the data.

When information hacked is coded as not criminally used this means the information had not been criminally used, or used to commit fraud at the time of the news coverage. In other words, this variable does not take into consideration if stolen information was criminally used later on. So it is also possible that a greater percentage of information stolen either has been, or will at some point, be used in a criminal way. For the variable called

time which refers to the time it took a victim to respond to an incident after learning about it, it is likely that the category more than a week is under representative and the category no response is over represented. Again this is because only information available at the time of the news coverage can be taken into consideration. So if a victim responded after that then they would be coded as no response at all when they should really be coded as taking more than a week to respond.

### Validity

Validity can be a big problem with secondary analysis or with using data from another source. In order to minimize this threat all definitions must be carefully developed. All variables in this project are operationalized in the section titled variables. The variables are designed to test the complex system and moral panic perspectives. Hacker skill level, notoriety, locus, nature of breach, and the rest of the variables test these two perspectives. However the eleven variables used in this study are not a comprehensive test of the moral panic and complex system perspectives. There are other ways to test these perspectives that are not used. For example the moral

panic perspective could be tested by compiling a sample of news articles and news coverage over identity theft incidents and seeing how often the people involved think this crime is unstoppable. A variable such as this could not be included in this study because the thoughts of victims were not covered in many of the cases included in the ITRC's data base. Some other ways to test these two perspectives that were not applied in this study are mentioned under the recommendations for future research section.

#### Sample Description

Table 2 reports descriptive variables of the sample. The first one is the various sources that the ITRC obtained case information from; 54.55% of the cases included in the ITRC data set were covered by a credible news article. Letter's to the Attorney General was the next most common source representing 28.94% of cases.

In regards to region, past literature indicates that the northeast is the region with the most identity theft (Federal Trade Commission, 2000). In the current study, the northeast is not responsible for a majority of identity theft cases. This is a sign of a good sample and that no

one region is significantly overrepresented in the data set.

Table 2. Descriptive Variables

Source	Frequency (N)	Valid Percent
company website	21	3.18%
HHS website	69	10.45%
hospital website	6	0.90%
letter to AG	191	28.94%
News article or spot	360	54.55%
Report to Congress	2	0.30%
school website	7	1.06%
US Attorney's office	4	0.60%
Region	(493)	
Central	11	2.23%
East	100	20.28%



North	28	5.68%
Northeast	82	16.63%
Northwest	40	8.11%
South	60	12.17%
Southeast	86	17.44%
West	86	17.44%

### Variables

The data set used for this study was created using content analysis of information provided by the ITRC. Three groups of variables were generated for this study; Appendix A describes the definitions and coding used for all variables. The first group of variables contains the two variables designed to capture aspects of the complex systems perspective. The second group contains the seven variables that were designed to capture the concepts used to test the assumptions of moral panic. The final group consists of the two dependent variables. In all there are eleven variables in these three groups.

Descriptive statistics for the eleven variables used in this study are provided in Tables 3-5. Some of the

variables are not completely consistent with items used in prior research. For example in past studies it was possible to count the number of identities that were actually used to commit fraud enabling the researcher to calculate the percent of stolen identities that were actually used criminally. Unfortunately, the data used for this project does not provide the exact number of frauds that have occurred from each security breach in very many cases. The source only mentions if fraud was committed, and thus, a variable called use of information was used.

The variable called skill level is broken down into two different skill levels; advanced computer skills required, and minimal computer skills required. Advanced computer skills are things like the ability to read encrypted data, hack into secure networks, or get passed computer security. Minimal computer skills involves breaches that do not require hacking secure sites, or only the hacking of a non-secure site or a single password or simply writing down social security numbers that were accidentally left on the computer screen by an employee.

Notoriety describes the scope of the breach. There are four categories; local which means only people from one city were affected, regional includes incidents involving

two or more cities but in the same state, national cases involve two or more states, and international indicates that people from two or more countries were affected by the breach. The variable locus of violation breaks down breaches into three categories; those committed by employees, outside hackers with inside help, and outside hackers alone. The variable nature of breach classifies breaches into paper or electronic.

The variable organization response breaks down all victim responses into five categories. First there is notify those who might have been affected by the breach, then notify law enforcement, notify the attorney general, public notice or public announcement, and lastly two or more responses. The variable time refers to the time an organization responded to a breach after becoming aware of it. The two responses are: responded within a week, and took more than a week to respond. Victim type refers to the type of organization victimized. The four types are business, education, medical, and military/government. The variable called records exposed by breach type refers to the number of incidents by breach. For this variable there are four types of breaches, employee theft, administrative error, missing or stolen hardware, and outside hacker.

The variable law enforcement response is coded as yes law enforcement responded to an incident or as no law enforcement did not respond to the incident. In order for this variable to be coded as yes law enforcement must have done something more than take a report. The variable exposed has no coding, it's the number of personal records exposed for each breach.

Table three below shows descriptive statistics about the complex system perspective. Table four is about the moral panic perspective. Table five is about the dependent variables. Table 3 first shows the employee status of offenders. In 50.85% of all 2010 identity theft cases the offender was an employee from within the organization that was victimized. In 7.91% of cases the offender was not an employee of the organization victimized but had help from someone who was. In 40.24% of cases the offender had no affiliation with the victim and was considered to be an outside hacker working alone or not working with anyone from within the organization.

Table 3 also shows that only 2.28% of identity theft cases in 2010 that were included into the ITRC data set were international. This is likely due to the ITRC's collection criteria. For example, in order for the ITRC to

include a case in the data set it must have been covered in an American-based source. Therefore, the number of international cases included in this study is vastly under representative of the total number of international identity theft cases in the year 2010. A majority of cases (57.60%) were regional meaning that they affected people living in more than one city but only in one state. If a breach was coded as local it means that the breach only affected people living in a single city or in a smaller area than that. National cases mean that there were victims in two or more states and international means there were victims in at least two countries.

Table 3. Description of Complex Systems Measures

Locus	Frequency (N)	Valid Percent
Employee from within the organization	308	51.85%
Outside hacker alone	239	40.24%
Outside hacker with inside help	47	7.91%

Notoriety	(658)	
Local	132	20.06%
Regional	379	57.60%
National	132	20.06%
International	15	2.28%

As outlined in Table 4, moral panic was measured with seven variables. The first variable used is called nature of breach, classified as either electronic or paper: electronic breaches account for 80.48% of the cases captured in 2010. Notably the business/financial sector accounts for the most incidents of identity theft in 2010 representing 51.44% of the sample. The medical sector was next representing 23.00% of the sample. The military/government sector was third representing 15.43% of the sample.

The most common breach type was missing or stolen hardware which represents 29.51% of breaches. Employee from within the organization represents 28.41% of cases and outside hacker represents 27.94% of cases. Administrative error represents 14.13% of cases. It is noteworthy that

outside hacker, employee from within the organization, and missing or stolen hardware are each nearly 30% of the sample and administrative error represents roughly half that much or 15% of the sample.

Table 4 also shows whether or not information stolen or records exposed was ever criminally used or used to commit a crime. In 87.50% of cases personal information stolen was not used to commit fraud or in any other criminal way. In 12.50% of cases stolen personal information was used to commit fraud or in some other criminal way.

In order for an incident to be coded as a yes for law enforcement response, law enforcement must have done more than simply take a report about the crime. In other words law enforcement must have made an arrest or somehow put in more effort to solve the crime than simply take a report about the incident. Law Enforcement responded just under a fifth of the time or in 19.61% of cases.

Organization response describes the action taken by victims. The most common action taken by victims of this crime was to notify law enforcement; 36.32% of victims notified law enforcement and took no other action at the time that the ITRC learned about the case. Notify the

Attorney General was the next most common action taken by victims and 29.37% of victims notified the Attorney General's office. The third most common action taken by victims was to have two or more actions or for example notify law enforcement and those affected by the crime or notify the Attorney General and law enforcement, and 18.08% of victims took two or more actions. Just 13.76% of victims notified those believed to be affected by the crime and left it at that. Only 2.47% of victims took no action at all. 84.57% of victims responded within a week of learning that they had been victimized. Only 15.43% of victims waited more than a week to respond but still responded to being victimized.

Table 4. Description of Moral Panic Measures

Nature of Breach	Frequency (N)	Valid Percent
Electronic	532	80.48%
Paper	129	19.52%
Victim Type	(661)	
Business/Financial	340	51.44%



Education	67	10.14%
Medical	152	23.00%
Military/Government	102	15.43%
Records Exposed by Breach Type	(637)	
Administrative error	90	14.13%
Employee from within organization	181	28.41%
Missing or stolen hardware	188	29.51%
Outside hacker	178	27.94%
Criminal Use	(648)	
No	567	87.50%
Yes	81	12.50%
Law Enforcement Response	(617)	
No	496	80.39%
Yes	121	19.61%
Organization Response	(647)	
None	16	2.47%

Notify AG	190	29.37%
Notify LE	235	36.32%
Notify those affected	89	13.76%
Two or more actions	117	18.08%
Time	(622)	
More than a week	96	15.43%
Within a week	526	84.57%

The first dependent variable for the study is called exposed. This stands for the number of personal records exposed in each case. This is a continuous level variable that is coded as the exact number of records exposed for every identity theft incident included into the ITRC dataset for the year 2010.

Skill level is coded into two different skill levels or types of identity theft; high-tech and low-tech. Low-tech incidents are things like finding social security numbers in a trash can or finding information online that was made publically available, or stealing information from a computer that is not encrypted or that is only protected

by a single password. High-tech incidents involve complex hacking skills for example the hacking of a relatively secure website or a computer with virus protection. The data shows that 81.99% of identity theft incidents in 2010 were low-tech crimes while 18.03% of identity theft incidents were high-tech.

Table 5. Dependent Variable

Skill Level	Frequency (N)	Valid Percent
High-Tech	119	18.03%
Low-Tech	541	81.99%

## CHAPTER FIVE

### RESULTS

This chapter talks about the hypothesis tests. Hypothesis one and two address the complex systems perspective. Hypotheses three through nine address the moral panic perspective.

#### Complex Systems Hypotheses

Hypothesis one uses a variable called skill level which is a categorical variable with two responses and the variable notoriety. This variable is also categorical and there are four responses to it. Therefore a 2x4 table is used and a Chi-Square analysis. Table 6 below shows the results of hypothesis test one.

Table 6. Hypothesis Test 1

	High-tech	Low-Tech	Cramer's V	Chi-Square	Sig
Local	11.86% (14)	21.89% (118)	.232	35.469	.000

Regional	48.31% (57)	59.55% (321)			
National	32.20% (38)	17.44% (94)			
International	7.63% (9)	1.11% (6)			

Cramer's V value is .232 for hypothesis one which means the relationship between the variables is weak to moderate. This relation is highly significant ( $p < .01$ ). Also the expected frequencies are greater than the observed frequencies for low-tech international cases. This is likely due to an incomplete sample of international cases; therefore it is likely that the findings for international cases in this study are not that generalizable due to a sample size consisting of only 15 international cases.

There were more high-tech international cases than expected. This should not be a big surprise. It is often more difficult to hack into a database that is large enough to contain personal information for people all around the country than it is to hack into a smaller database

containing only a few names. This is because bigger databases have more to loose and therefore are more likely to be protected with more security. Again this finding may not be all that generalizable due to a small sample size in this category.

Hypothesis two examines the locus of the violation which accounts for who committed the attack. Locus of violation is a categorical variable with three categories. The variable hacker skill level is also used and this variable is also categorical with two possible responses. Therefore a 3 by 2 contingency table was used and the Chi Square test of independence. Cramer's V was the measure of association used. Table 7 below shows the results for hypothesis test two.

Table 7. Hypothesis Test 2

	High-tech	Low-tech	Cramer's V	Chi-Square	Sig
Employee	0.88% (1)	63.69% (307)	.526	164.645	.000
Outside	7.02%	8.30%			

hacker with inside help	(8)	(40)			
Outside Hacker	92.11% (105)	28.01% (135)			

Cramer's V is .526 which means the relationship between the variables is moderate to strong. The Pearson's Chi-Square value is 164.645 for hypothesis two. The relationship between the variables is statistically highly significant ( $p < .01$ ). The most significant finding here is that outside offender alone are more likely to commit high-tech breaches while outside hackers with inside help and inside employees are more apt to commit low-tech breaches. Also high-tech breaches are rarely the result of employees from within an organization, yet employees account for 51.68% of all identity theft breaches. Overwhelmingly most of those breaches are low-tech.

### Moral Panic Hypotheses

Hypothesis three considers two categorical variables. First hacker skill level is measured as high-tech or low-tech hacker, and nature of breach is measured as electronic or paper identity theft. Table 8 below shows the results of the chi-square analysis.

Table 8. Hypothesis Test 3

	Low-tech	High-tech	Phi	Chi-Square	Sig
Paper	22.41% (119)	0% (0)	.231	35.27	.000
Electronic	77.59% (412)	100.00% (129)			

A Phi coefficient of .231 is slightly less than .290 suggesting that the relationship between the variables is weak to moderate, and no breaches were both paper and high-tech (sig .000). After coding all the cases it became apparent why no cases fell under this category. Paper breaches were incidents like a file cabinet filled with



social security numbers being sold at a garage sale or an employee who stole paper files on customers from their employer or other things like that. In order for a breach to be considered high-tech it must have required some advanced computer skills such as the hacking of a computer protected by more than one password or encrypted data or something along those lines. About 18% of cases involved paper hacking and all of these cases were also low-tech. There were 412 low-tech electronic breaches. So a total of 80% of cases were low-tech. This means that 20% of breaches were electronic and high-tech.

Hypothesis four uses the variable law enforcement response which is a categorical variable with two possible responses. The other variable used is called victim type. This is also a categorical variable and there are four possible responses. A 4x2 contingency table was used along with a Chi-Square analysis. Table 9 below shows the results for hypothesis test four.

Table 9. Hypothesis Test 4

	Bus	Edu	Med	Mil/Gov	Cramer's V	Chi- Square	Sig
No	80.88% (220)	89.06% (57)	80.44% (37)	68.82% (64)	.149	10.475	.015
Yes	19.12% (52)	10.94% (7)	19.56% (9)	31.18% (29)			

Cramer's V is .149 for hypothesis four so the relationship between the variables is weak in this case. The obtained Pearson's Chi-Square value is 10.475. The significance level obtained is .015 which is less than .05 but greater than .01 so the relationship is significant but not highly significant. The main finding here is that law enforcement does not appear to be responding to a majority of breaches regardless of what category the victim falls into. However the relationship between the variables is weak so this finding cannot be said with much certainty. On average police only responded in 20.00% of breaches.

Hypothesis five uses the variable exposed which is a continuous variable. Hypothesis five also uses the variable victim type which is a categorical variable with four

possible responses. Exposed is the dependent variable. With one categorical and one continuous variable an ANOVA analysis was used for hypothesis five. Table 10 below shows the results for hypothesis test five.

Table 10. Hypothesis Test 5

	Mean (SD)	Eta	F	(df)	Sig
Business/Financial	22,981.46 (211,129.62)	.108	1.973	507	.117
Education	25,783.99 (96,278.04)				
Medical	93,390.29 (402,624.05)				
Military/Government	11,898.36 (35,551.75)				

The findings for hypothesis five are not significant at an alpha level of .05. Therefore it can be assumed that no relationship exists between the variables exposed and victim type. Hypothesis five does not offer strong support for the moral panic perspective.

Hypothesis six involves the variable records exposed by breach type and nature of breach. Nature of breach is a categorical variable with two possible responses; paper or electronic. The variable called records exposed by breach type is a categorical variable and there are four different breach types. With two categorical variables, a Chi-Square test of independence is used for hypothesis six along with Cramer's V. Table 11 below shows the results for hypothesis test six.

Table 11. Hypothesis Test 6

	Empl	Admin	Stolen	Outsid e Hacker	Cramer 's V	Chi- Squar e	Sig
Paper	28.79 % (76)	53.13 % (17)	12.77% (6)	4.71% (13)	.362	81.13 0	.00 0
Electroni c	71.21 % (188)	46.88 % (15)	87.23% (41)	95.29% (263)			

Cramer's V value is .362 for hypothesis six meaning that the relationship between the variables is moderate. A Pearson's Chi-Square value of 81.130 was obtained for hypothesis six. The relationship between the variables is highly significant. Also notably employee theft is more likely to be paper than the expected frequencies show and breaches resulting from outside hackers are more likely to be electronic than the observed frequencies show. These findings do mean something because the relationship between the variables is moderate and highly significant. Furthermore paper breaches are much more likely to result from inside employees than administrative errors, outside hackers, and missing or stolen hardware combined. Electronic breaches are primarily outside hackers and employees.

Hypothesis seven used the variable records exposed by breach type which is a categorical variable with four categories and the variable called exposed which is a continuous variable. The variable called records exposed by breach type is the independent variable and the variable called exposed is the dependent variable. There are four different breach types and the number of records exposed is

a continuous variable; an ANOVA analysis was used. Table 12 below shows the results for hypothesis test seven.

Table 12. Hypothesis Test 7

	Mean (SD)	Eta	F	(df)	Sig
Employee theft	33,229.71 (269,322.31)	.065	.862	617	.460
Administrative error	61,995.78 (233,198.11)				
Missing or stolen hardware	3,621.40 (6,275.28)				
Outside hacker	18,239.04 (82,522.69)				

Hypothesis seven shows that there is no significant relationship between the variables records exposed by breach type and exposed. All the findings here are insignificant at an alpha level of .05. This hypothesis does not confirm any relationship between the two variables

and therefore does not offer strong support for the moral panic perspective.

Hypothesis eight uses the variable criminal use which is a categorical variable with two responses. Also the variable called exposed is used. This is the dependent variable and it is continuous in nature. Therefore an ANOVA analysis is used. Table 13 below shows the results of hypothesis test eight.

Table 13. Hypothesis Test 8

	Mean (SD)	Eta	F	(df)	Sig
Yes info used criminally	3,087.05 (19,412.92)	.042	1.155	646	.283
No info not used criminally	26,998.54 (198,775.30)				

The findings for hypothesis eight were not significant at an alpha level of .05. Therefore no significant relationship can be established or confirmed between the

variables exposed and criminal use. It does appear that most of the records exposed are not criminally used but this finding cannot be confirmed with much certainty because the relationship between the variables is weak and not significant.

Hypothesis nine uses the variable organization response which is a categorical variable with five categories and the variable time it took organization to respond after incident. This variable is also categorical and has two categories. Therefore a 5x2 table was used along with a Chi-Square analysis and Cramer's V. Table 14 below shows the results of hypothesis test nine.

Table 14. Hypothesis Test 9

	Within a week	More than a week	Cramer's V	Chi-Square	Sig
Notify those affected	12.05% (63)	25.00% (24)	.216	28.808	.000
Notify LE	37.48%	33.33%			



	(196)	(32)			
Notify AG	33.08%	13.54%			
	(173)	(13)			
Public	16.83%	25.00%			
notice	(88)	(24)			
Two or	0.57%	3.13%			
more	(3)	(3)			
responses					

A Cramer's V value of .216 is obtained which means the relationship between the variables is weak to moderate. A Pearson's Chi-Square value of 28.808 is obtained for hypothesis nine. The relationship between the variables is highly significant. Notably when the only action taken by an organization is to notify those people who might have had their records compromised, the response is more likely to take more than a week than expected. When an organization responds by notifying the Attorney General the response is more likely to occur within a week than expected. If an organization responds with two or more responses, then it is more likely that these responses will

take more than a week to occur than expected. These relationships are weak and can mostly be explained. Notifying thousands of people takes more time than making a single phone call to the Attorney General's office and two responses takes longer to do than one. It is notable that the category for two or more possible responses has a small number of cases. Only six cases fell into this category. This is likely due to the news coverage of identity theft incidents. If a company responded by sending out letters to those affected and by notifying law enforcement it is possible that news stations would simply report that notifications were sent out to those affected and they would consider that as sufficient coverage.

## CHAPTER SIX

### DISCUSSION

In this chapter the results of the hypothesis tests are examined in reference to prior literature, specifically, the policy implications for the complex systems and moral panic perspectives are considered. Specific limitations of this project that may have affected the results are addressed. Recommendations for future research are then made. The chapter concludes with policy implications.

#### Complex Systems

Hypothesis 1 and 2 offer some support for the complex systems perspective. If security systems today were getting more and more complex and interconnected all of the time the first sign would be that national and international cases are more prevalent and high-tech compared to the past. This finding is observed but the evidence of it in international cases is weak. Again the limitations of the data, namely the small sample size of international cases can likely explain this. Past studies have indicated that breaches large in scope are on the increase (Zhu, Security

control in inter-bank fund transfer, 2002). This finding appears to be consistent with the findings of the current study.

The findings also show that there is a moderate to strong relationship between the variable skill level and locus. Specifically, high-tech breaches are overwhelmingly more likely to be the result of outside hackers working alone rather than employees or an outside hacker with inside help. If systems were getting more and more complex one would expect to see this because it should be harder and harder to hack into ever more complex systems, therefore it would be more time consuming and harder to do at work. Therefore professional hacker groups (which are almost always outside hackers with no ties to their victims) should account for a greater proportion of high-tech breaches and breaches in general. This is sort of observed, but the most common type of breach is still low-tech breaches by inside employees. This is likely because there are still more opportunities for easy breaches by inside employees than there are for anyone else. In the past a larger percentage of breaches fell into the low-tech employee category (Erickson & Howard, 2007).

### Complex Systems Recommendations for Future Research

There were inconsistent results regarding the complex systems perspective. Future research on the topic should strive for a much larger sample size of international cases than in the present study if results are to be generalizable for international cases. Also, future research should use a larger range of indicators in those signs presented in this study. For example in a world with evermore complex online security systems one would expect more and more organizations (especially large ones) to hire people whose job is solely to guard against identity theft and cyber-attacks. The presence of a dedicated, highly trained security department and the examination of data storage protocol are necessary. In addition if outside hacker groups are becoming more specialized in the types of hacking jobs they attempt, their success rates should also be examined. Future research should look more closely at organizational responses following victimization by outside hackers, and preventative strategies that specifically target outside hackers. A longitudinal study that looks closely at the changing trends in this crime and compares them over time could yield some important results. These

results may lead to more policy implications and/or confirm the ones made in this study.

### Complex Systems Policy Implications

The research still shows that inside employees are responsible for just over 50% of identity theft breaches and they predominately resort to low-tech means. Therefore companies, businesses, and organizations should tighten up the security of their employees, and minimize who has access to personal information. Larger organizations that hold more valuable information or more personal records should especially consider this and consider hiring an online security expert specifically to guard against identity theft and other cyber-attacks. Organizations themselves can make a difference and put a huge dent in identity theft. For example organizations need to destroy dated information on the personal records of clients, customers, and employees alike (Prosch, 2009). This information often has a time frame in which it is useful to organizations but the same information never expires for identity thieves (Benson, 2009).

Since a sizeable amount of identity theft incidents are committed by high-tech outside hackers there is a need for all organization types to have a good online security

system. A network called SWIFT that is currently in use with some banks is a good (but not perfect) example of this. SWIFT connects banks and other financial institutions worldwide. Each customer of SWIFT (or financial institution) has one computer dedicated to SWIFT that has pre-accredited software with encryption, authentication, and data scrambling on it. This computer alone is connected to a network by a leased line owned by SWIFT. All messages are formatted and coded before being sent out to another financial institution using SWIFT. Different codes are used for different types of transactions, for example bank to bank transfers have a different code than customer to bank transfers or precious metal transfers do. Messages on each end must be authenticated by a valid user before they can be read. Also each bank has a unique part of the encryption system for every other bank they conduct business with (Zhu, Security control in inter-bank fund transfer, 2002).

However the algorithms that code messages do not prevent the messages from being duplicated, sent at a different time or even deleted. All algorithms really do is prevent information from being read without a code. Passwords are issued from SWIFT in two different parts in the form of tables. This prevents any one break in security

from being able to gain an entire password. Swift also has packet filtering which prevents any customer to customer traffic without going through SWIFT first. This prevents hackers with a way of hacking banks without going through SWIFT. Also Swift separates its different routers and information into domains so even if a hack attempt does get through it will only be into part of the system and the hacker will need to break even more codes before getting access to other parts of the SWIFT system (Zhu, Security control in inter-bank fund transfer, 2002).

SWIFT's major weakness is that it provides attackers with the ability to modify, intercept, or delete messages. Zhu (2002) recommends that SWIFT gets better link to link encrypting. This would encrypt messages with a public key code at the other side of the link. In other words a sending bank would use three different types of encrypting codes, and then convert the message into cipher text and send the message to an operating center. That operating center would send the message to another operating center which would send the message to the receiving bank and then the receiving bank would decode it (Zhu, Security control in inter-bank fund transfer, 2002). The point is that SWIFT is not perfect but it is an example of a sophisticated



online security system that has had some success in guarding against high-tech identity theft and fraud in banks. A system like this would be a good step to guard against high-tech online hacking incidents.

Mandatory reporting laws for all types of identity theft would also be a good idea. If nothing else, this would help to reveal the true extent of the problem of identity theft. Such laws would also give law enforcement an advantage and ideally an early alert system as well. It is impossible for law enforcement to react to a crime that they don't know happened. Some such laws already exist but often they are incomplete. For example, Minnesota state law mandates that anytime someone steals personal information electronically from a business the business has to inform those that might be affected. The law does not mandate that businesses do the same if the data is stolen in a manner that is non-electronic (Data breach illustrates disclosure disparity, 2011).

In 2011, a company in Nashville Tennessee had a laptop computer stolen from a room in company headquarters that only employees of that company had access to. This laptop contained the full names, driver's license numbers, and social security numbers to some of the company's clients.

The company promptly notified the Attorney General's office and local law enforcement. They also sent out a letter notifying those affected by the breach and offering them free credit monitoring services for two years. In addition, the company installed new training practices and procedures and a system of checks and balances for current employees and hired a private investigator to try to recover the laptop. Consequently, the company has not been the victim of identity theft since and so far no fraud has been committed using the identities stolen in the incident (Identity Theft Resource Center, 2011). This is a good example of the types of steps companies should take after being victimized by identity thieves along with some preventative measures that companies should do as indicated by the findings in this paper.

### Moral Panic

Hypothesis three through nine offer some support of the moral panic perspective but the results are somewhat mixed. Hypothesis three shows a weak to moderate relationship between the variables nature of breach, and hacker skill level. High-tech breaches are much more apt to be committed through electronic means. Paper breaches are

low-tech. This relationship is highly significant.

Hypothesis six shows that outside hackers account for more electronic breaches than any other breach type. Employees account for the second most electronic breaches and the most paper breaches. Administrative error and missing or stolen hardware are responsible for much less breaches than outside hackers and employees. This relationship is moderate and is highly significant.

In the past employees were the most common breach type and they accounted for almost twice as many breaches as outside hackers working alone (Erickson & Howard, 2007). Perhaps this is an early indication that the crime of identity theft is becoming more polarized than ever before. It appears that a large portion of breaches are electronic and committed by outside hackers or paper and committed by employees. Also electronic crimes are more likely to be high-tech as indicated in hypothesis three. On one hand, high-tech outside hackers are responsible for more identity theft than before compared to prior findings and on the other hand inside employees are committing more low-tech breaches. The middle grounds seem to be disappearing.

Hypothesis seven shows no sufficient evidence that any one type of breach exposes significantly more personal

records than another. The results showed no significant difference in the number of records exposed between employees, administrative error, missing or stolen hardware, and outside hackers. The relationship was not significant even at an alpha level of .05. The standard deviations were quite high in this hypothesis, possibly indicating a large concentration of outliers. If these outliers are disregarded the relationship becomes more significant. Past literature has indicated that a few years ago employees accounted for more records exposed than other breach types, but a changing trend with outside hackers being responsible for more and more records exposed was previously acknowledged (Erickson & Howard, 2007).

Hypothesis five shows no significant relationship between victim type and the number of records exposed. The business/financial sector, education sector, medical sector, and government/military sector are not responsible for a significant difference in the number of records exposed. The relationship between these two variables is insignificant even at an alpha level of .05. The standard deviations were also quite high in this hypothesis indicating some outliers in the sample. Past literature has clearly indicated that the business sector is responsible

for a considerably higher number of personal records exposed than the other sectors (Erickson & Howard, 2007).

Hypothesis four, eight, and nine offer some support for the moral panic myth that identity theft is seen as unstoppable and unsolvable and therefore organizations and law enforcement are not likely to respond to identity theft breaches. Hypothesis four found a weak relationship between the variable law enforcement response and victim type. Hypothesis four shows that in 80.00% of identity theft cases law enforcement does not respond at all. Past literature has indicated that law enforcement is not likely to respond to identity theft cases in any way beyond simply taking a report and that most law enforcement agencies nationwide do not poses the time, training, or resources to deal with this crime (Gogolin & Jones, 2010). This is suggestive that identity theft is seen as unstoppable/unsolvable and therefore, not many resources are put into it and law enforcement often does not respond to such cases.

Hypothesis eight used the variables criminal use and records exposed. Hypothesis eight found no significant relationship between the variables. Again the standard deviations were quite high indicating the presence of

outliers. Most of the time personal records are exposed they are not used to commit fraud or in a criminal way at all. This finding suggests that identity theft is mostly not the result of malicious hackers. It could also mean that identity theft breaches are now more apt to be employees without malicious intent. Past statistics indicate that employee types of fraud are the most common (Federal Trade Commission, 2009). Identity theft appears be predominately inside employees who either do not know how to use the information they steal most of the time or for whatever reason do not use that information to commit fraud very often.

Hypothesis nine used the variables organization response and time it took to respond after incident. The relationship between these variables was found to be weak to moderate and highly significant. Each type of response is much more likely to happen within a week of the organization finding out about a breach than to happen in more than a week with one exception. The exception is if an organization responded in two or more ways, in this case they were equally as likely to respond within a week as they were to respond in more than a week. The sample size in this category was quite small, plus it is possible that

the news coverage said it took these organizations longer than a week to respond, when they really meant it took them longer to finish responding. For example, if an organization notified law enforcement and half of those affected within a week but took a few extra days to finish notifying those affected it might have been coded as taking more than a week to respond. Similarly, some organizations could have responded in a second way after the news coverage but still been coded as only responding in the way they did first. This finding does not support a myth that identity theft is perceived as unstoppable and therefore there is no reaction to it. When organizations do respond to identity theft they tend to do so promptly or within a week of discovering the breach.

#### Moral Panic Recommendations for Future Research

Future research on this topic should look into the size of organizations that are being victimized by identity thieves and look for a relationship between organization size and victimization. The ITRC and the majority of news articles contained in their data base did not mention the size of the organization victimized. Therefore organization size could not be used in this study. In addition future research should look into the possible polarizing of

identity theft. It seems as though a greater percentage of breaches are high-tech outsiders or low-tech employees and there does not appear to be much of a middle ground.

Future research should take a close look at different types of organization responses and their corresponding success rates for solving the crime. At this point this would be more exploratory research than anything else because the literature up to this point does not really show that any one response produces more favorable results than any other, but anytime the trends of a crime change it might pay off to take another close look at the phenomenon as a whole.

#### Moral Panic Policy Implications

Instances of high-tech electronic breaches seem to be on the rise. This finding indicates a pressing need for better more secure firewalls and virus protection on company computers. Since instances of high-tech breaches are on the rise it would appear that whatever preventative strategies we have in place to prevent hackers from wanting to hack are not working. Therefore it is imperative that physical limitations to the ability to hack such as firewalls and electronic security be strengthened both on business and on personal computers (Federal Trade



Commission, 2003). By extension there is a growing need for organizations to have their own electronic security professional. Organizations, especially larger ones might want to look into hiring such people.

Perhaps a more efficient preventative strategy that organizations should also employ to prevent identity theft is to limit who within the organization has access to this kind of information, and keep closer tabs on employees (Ward, 2003). The study at hand found that employees are still responsible for the most incidents of identity theft. This finding is consistent with past literature and has been confirmed in other studies as well (Erickson & Howard, 2007), (Federal Trade Commission, 2009). Organizations could require each employee to swipe a unique ID card whenever using a company computer which would allow the organization to track who is using what computer and who has access to what information and when. This could prevent some employee identity theft and fraud.

Recently an employee from the state of Alabama was indicted on 15-counts of wire fraud, computer fraud, and aggravated identity theft. The employee used personal identities attained from a computer while at work in order to file for tax refunds. This employee was arrested as part

of a recent federal crackdown on identity theft and on tax fraud. The justice department is now working hand in hand with the IRS to investigate, prosecute, and punish identity thieves (United States Department of Justice, 2012). This case is a good example of a reason for employers to keep closer tabs on their employees. In addition it illustrates how effective law enforcement agencies can be at fighting identity theft when they have people trained in specific areas such as tax fraud. This case is a good example of different organizations successfully collaborating and helping one another out. The Justice Department and the IRS had to successfully work together to solve this case. It is imperative that organizations be able to work together in order to solve identity theft crimes. This is due to the potential high-tech and cross-jurisdictional nature of this crime.

Law enforcement has been found to not respond to most identity theft cases even though most breaches are from employees within the organizations victimized. Also most breaches are low-tech. Law enforcement agencies around the nation should consider training at least one police unit to handle this type of crime. Since this crime is still predominately low-tech in nature specially trained law

enforcement units should be able to make a difference. Currently, 42% of law enforcement agencies around the nation do not have a computer crimes unit and only 40% of new officers receive some form of training in this area; there are currently no known training options available for existing officers in this area (Gogolin & Jones, 2010). Having even one officer trained in electronic identity theft prevention for every jurisdiction could significantly reduce electronic identity theft, even if that officer was not trained to deal with high-tech breaches.

## CHAPTER SEVEN

### CONCLUSIONS

This project was meant to test two identity theft perspectives. One was the moral panic perspective. A myth that identity theft is an unstoppable crime that's mainly committed by high-tech outsider hackers was tested as well. The myth that identity theft is perceived as unstoppable and therefore victims and law enforcement frequently do not react to it was also tested. A complex systems perspective was tested too. The myth regarding complex systems that says systems are getting more complex and interconnected and therefore breaches are becoming more rare, devastating, and are having further reaching affects was tested as well. In addition current trends in identity theft were explored.

Commonly held perceptions about identity theft were compared and tested. Past research and this project offer some support of the moral panic perspective. One of the strongest forms of evidence found in this study that supports the moral panic perspective is the moderate to strong and highly significant relationship between outside hackers and high-tech breaches. On the flip side of that same relationship was the link between employees and low-

tech breaches. Outside hackers are significantly more likely to commit identity theft breaches that are high-tech in nature compared to employees. There is strong support of a polarization effect in this crime. High-tech outsiders and low-tech employees are the two dominant groups of offenders. Another finding that supports the moral panic perspective is the moderate and highly significant relationship between nature of breach and skill level. Electronic breaches are predominately high-tech while paper breaches are low-tech. Therefore the myth about the rise of the high-tech outside hacker is supported. One more characteristic can be added to that high-tech outside hacker and that is electronic. These hackers are using electronic means.

There was no significant relationship between the variables criminal use and records exposed. So the size or number of records exposed in a breach had no influence over whether fraud was committed or not. Also fraud was not committed in most identity theft cases. This suggests that high-tech hackers are not predominately motivated by money, but by other things. The relationship between the variables exposed and victim type was also not significant. This study did not find any significant difference in the number

of records exposed in the business, education, medical, or military/government sectors. More than anything this finding shows identity theft is not a problem with any one sector rather it is a potential problem in every organization.

### Final Statements

Probably the most significant finding to come from this research is the polarization of identity theft in recent years. High-tech outside hackers and low-tech employees account for most identity theft cases. Therefore a core policy implication is that any sound identity theft security system for any organization type needs two parts. First it needs a good way to keep tabs on employees and track their use of company computers. Secondly a secure online security system to guard against outside hackings is needed.

United States law enforcement in general is ill equipped to handle identity theft cases and consequently they only take a report in 80% of identity theft incidents. A majority of identity theft incidents are the result of employees resorting to low-tech means. The incident where an employee in the state of Alabama was indicted is a good

example of this. In that case a state employee used a work computer to steal people's identities using low-tech means. This employee was indicted as a result of the collaboration of the IRS and the Justice Department (United States Department of Justice, 2012). Consequently if more law-enforcement agencies even had a unit only trained to respond to low-tech identity theft crimes then a significant amount of identity theft cases should be solvable. In theory incidents of identity theft will then reduce along with moral panic over this crime.

APPENDIX A  
VARIABLES



Perspective/Concept	Variable	Definition	Coding
Complex Systems/Scope of breach	Notoriety	extent to which the incident effected people	1-only local people effected 2-people effected in the entire region 3-people effected all over the nation 4- people internationall y effected or two or more countries effected
Complex Systems/Locus of violation	Locus	Status of perpetrator	1-employee from within the organization 2-outside hacker with inside help 3-outside hacker alone .-unknown
Moral Panic/Method of attack	Nature of breach	Instances involving paper or a hard copy of someone's personal information are considered paper the use of a computer is electronic.	1-paper 2-electronic .-unknown

Perspective/Concept	Variable	Definition	Coding
Moral Panic/Fraud or criminal use of information	Criminal use	At least one person's personal information was used in a criminal way (or if fraud was committed) or not.	1-yes 0-no .-unknown
Moral Panic/Action taken by victim	Organization response	How organizations respond to a security breach.	1-responded by notifying those whose records might have been compromised 2-responded by notifying law enforcement 3-responded by notifying the Attorney General 4-public notice 5-two or more of the above response types/public notice and another response .-unknown
Moral Panic/Time it took organization to respond after incident	Time	time it took organization to respond to a breach after it happened	1-within a week 2-more than a week .unspecified/no response at all

Perspective/Concept	Variable	Definition	Coding
Moral Panic/Sector or type of victim	Victim type	the number of identity theft incidents in the year 2010 by sector	1-business 2-education 3-medical 4-military/ government
Moral Panic/Number of incidents by breach type	Records exposed by breach type	This variable accounts for the number of identity theft incidents per breach type.	1-employee theft 2- administrative error 3-missing or stolen hardware 4-outside hacker .-unspecified breach
Moral Panic/Response by a law enforcement agency	Law Enforcement response	This categorical variable accounts for whether law enforcement looked into an incident or not.	1-yes 0-no .-unknown

Perspective/Concept	Variable	Definition	Coding
Dependent variable/Hacker skill level	Skill Level	Breaches involving online hacking require high-tech hacker skills stealing unencrypted information requires low-tech skills.	1-advanced computer skills required (high-tech) 2- minimal technical skill required (low-tech) .-unknown
Dependent variable/Number of records exposed	Exposed	Records exposed	No coding

## REFERENCES

- Data breach illustrates disclosure disparity. (2011).  
*Minneapolis St. Paul business journal*, 1-27.
- Bachman, R., & Paternoster, R. (2004). *Statistics for criminology and Criminal Justice*. Prentice Hall.
- Benson, M. (2009). Offenders or opportunities: Approaches to controlling identity theft. *Criminology public policy*, 231-236.
- Collins, J. (2003). Business identity theft: the latest twist. *Journal of Forensic Accounting*, 303-306.
- Erickson, K., & Howard, P. (2007). A case of mistaken identity? news accounts of hacker, consumer, and organizational responsibility for compromised digital records. *Journal of Computer-Mediated Communication*, 1229-1247.
- Federal Trade Commission. (2000). *Identity Theft information*. Retrieved from ID Theft: When bad things happen to your good name:  
<http://www.popcenter.org/problems/identitytheft/3>
- Federal Trade Commission. (2003). *Identity Theft survey report*. Retrieved from Investor Solutions:  
<http://www.investorsolutions.com/news/356/15/Protecting-Yourself-Against-Identity-Theft/>

Federal Trade Commission. (2009). *Identity Theft data*.

Retrieved from Identity Theft consumer complaint data:

<http://www.ftc.gov/>

Gogolin, G., & Jones, J. (2010). Law enforcement's ability to deal with digital crime and the implications for business. *Information security journal*, 107-109.

Hetu, D. (2011). Chit-Hack information exchange paths in IRC hacking chatrooms. (pp. 1-28). Montreal: University of Montreal.

Hetu, D., Morselli, C., & Langlois, S. (2011). Welcome to the scene: A study of social organization and recognition among Warez Hackers. *Journal of research in crime and delinquency*, 1-24.

Identity Theft Resource Center. (2010). *Data breaches in 2010*. Retrieved from Identity Theft Resource Center: <http://www.idtheftcenter.org/artman2/publish/libsurvey/Breaches2010.shtml>

Identity Theft Resource Center. (2011). *Data breaches in 2011*. Retrieved from Identity Theft Resource Center: <http://www.idtheftcenter.org/artman2/uploads/1/ITRCBreachReport201120120207.pdf>

Kapsidelis, K. (2011). *Breach exposes data at VCU*.

Retrieved from Richmond Times Dispatch:

<http://www2.timesdispatch.com/news/2011/nov/12/2/tdmain01-breach-exposes-data-at-vcu-ar-1453805/>

Katherine, B., Jackie, A., & Paul, S. (2008). "Credit card fraud: awareness and prevention". *Journal of financial crime*, 398-410.

Morris, R., & Longmire, D. (2008). Media constructs of identity theft. *Journal of Criminal Justice and popular culture*, 1-18.

Newman, G. (2003). Check and card fraud. *Center for problem-oriented policing*, 2-21.

Newman, G. (2004). The problem of identity theft. *Center for problem-oriented policing*, 1-25.

Newman, G., & McNally, M. (2005). Identity theft literature review. *National Institute of Justice*, 8-17.

Prosch, M. (2009). Preventing identity theft throughout the data lifecycle. *Journal of Accountancy*, 1-17.

Sandywell, B. (2006). Monsters in cyberspace: cyberphobia and cultural panic in the information age. *Information, communication & society*, 39-61.

Synovate. (2003). *Federal Trade Commission*. Retrieved from Identity Theft study report:

<http://www.popcenter.org/problems/identitytheft/PDFs/FTC2003a.pdf>

United States Department of Justice. (2012, January). *State of Alabama employee indicted for identity theft and tax fraud*. Retrieved from United States Department of Justice:

<http://www.justice.gov/opa/pr/2012/January/12-tax-088.html>

United States Federal Deposit Insurance Corporation.

(2011). *Phishing scams*. Retrieved from United States Federal Deposit Insurance Corporation:

<http://www.fdic.gov/consumers/consumer/alerts/phishing.html>

Waldman, M. (2006). Science to select papers for extra secure review process. *Nature international weekly journal of Science*, 658-659.

Wall, D. (2011). The organization of cybercrime in an ever-changing cyberthreat landscape. *Criminal Justice Networks Conference* (pp. 1-19). Montreal: University of Montreal.

Ward, S. (2003). 10 Ways to prevent identity theft. *Small Business Guide: Canada, About.com*. Montreal, Canada.

Zhu, D. (2002). Security control in inter-bank fund transfer. *Journal of electronic commerce research*, 15-22.



Zhu, D. (2011). Fraud/money laundering. *Journal of Accountancy*, 1-3.