Identity Theft

This thesis is submitted in partial fulfillment of the requirements for the degree of
Master of Philosophy

Judy D. Newton
Cardiff School of Social Sciences
Cardiff University

April 10, 2013

Identity Theft

This thesis is submitted in partial fulfillment of the requirements for the degree of
Master of Philosophy

Judy D. Newton
Cardiff School of Social Sciences
Cardiff University

April 10, 2013

ACKNOWLEDGEMENTS

I would like to thank the men and women who participated in this study. Their cooperation, dedication and knowledge made this thesis possible. There are numerous individuals who assisted with this study whom I wish to thank and will be forever grateful for their help especially my primary confidential informant, “Charlie Hustle.” A special thank you goes to my initial supervisor Michael Levi and my most recent supervisor Lesley Noaks. Even though Lesley Noaks has been assigned to my supervision for approximately one year her insight and supervision has been immeasurable. Michael Levi has been with me for the long haul and without his guidance and support this thesis would not be presented today. Elizabeth Renton, Administrator at the school of Social Sciences was instrumental in providing her professional and expert assistance when called upon. Elizabeth, you are assigned to the appropriate role as an administrator. Please, you must remain at the University for as long as practical. Every student needs your expert advice because you are like “the mother hen looking over all of us chickens.” The continuous support by my dear sister-in-law Vivian Newton, my nephew Keith Walcott, Lynda, Donte, Marilyn, Bill,, Marianne, Michael, Jacqueline Taubman and James McCutcheon provided the necessary support when I needed it most. My heart and appreciation is attached to my mother Dorothy. You have made too many sacrifices to mention and taught me the value of a good education. Finally, I will forever be indebted to my supportive, sincere, thoughtful and loving husband Richard (Richie) Baxt who provided the means, inspiration and paved the way so that I may fulfill my dream.

This thesis is dedicated to the victims who suffered economic and emotional loss due to the reprehensible behavior of fraudulent individuals.

SUMMARY

Recognized as one of the fastest growing crimes in the United States, identify theft has eluded customary, reactive systems of containment, due to its rapidly changing nature, the dependency upon legislative and corporate efforts and the perceptions of the law enforcement and the business industry, which minimizes its impact. The prevention strategies have been ill matched to the nature of the crimes or interceded after the crimes have been committed.

In order to institute comprehensive identity theft protection, including the conviction of the criminals, a system sensitive to the changing nature of the crimes, the access a criminal has to personal identifying data and one which is proactive in nature is needed.

Therefore, the purpose of this study was to explore the usefulness of *the routine activity theory* (RAT) in the understanding of identity theft. The interview data were analyzed to explore the perceptions of the stakeholders, their evaluation of the usefulness of the application of this theory, and to determine more effective identify theft protection.

Using an ethnographic paradigm, a cross sectional representation of the stakeholders, twenty five law enforcement professionals, offenders and victims were provided with five general and five specific to each group of stakeholders (interviews) and probing (conversations) inquires to determine the current state of practice and whether their responses supported that RAT would be advantageous in the containment of this crime.

The analyses of the data revealed that RAT would be useful in the understanding of identity theft, provide a framework to modify the state of practice from a retrospective analyses after a theft was committed, to preventive measures, and that no ample framework was present. Implementing RAT as a theoretical model would be more pragmatic and incorporate a more global approach to the standard of practice.

The confounding conditions, such as the guardedness of the disclosed information, the limited access to archival records, the offenders available for the study, and the lack of formative studies to systematize the data indicated that additional research is needed. These include: (1) categorization of the interview data into propositions, and (2) the benefits of educational programs for governmental and law enforcement officers using RAT as proactive system in the reduction of these crimes.

TABLE OF CONTENTS

Appendices:

LIST OF ABBREVIATIONS

AUSA	Assistant United States Attorney
BBB	Better Business Bureau
BIN	Bank Identification Number
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics (DOJ)
CCIPS	Computer Crime and Intellectual Property Section (DOJ)
CCMSI	Credit Card Mail Security Initiative
CDFO	Commercially developed credit freeze option
CMS	Centers for Medicare and Medicaid Services (HHS)
CRA	Consumer reporting agency
CVV2	Card Verification Value 2
DBFTF	Document and Benefit Fraud Task Force
DEA	Drug Enforcement Agency
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
FACT Act	Fair and Accurate Credit Transactions Act of 2003
FBI	Federal Bureau of Investigation
FCD	Financial Crimes Database
FCRA	Fair Credit Reporting Act
FEMA	Federal Emergency Management Agency
FRB	Federal Reserve Board of Governors
FSI	Financial Services, Inc.

FTC	Federal Trade Commission
FTC Act	Federal Trade Commission Act
GAO	Government Accountability Office
GLB Act	Gramm-Leach-Bliley Act
HHS	Department of Health and Human Services
HIPPA	Health Insurance Portability and Accountability Act of 1996
IACP	International Association of Chiefs of Police
IAFCI	International Association of Financial Crime Investigators
IC3	Internet Crime Complaint Center
ICE	Immigration and Customs Enforcement (DHS)
IG	Inspector General
IRS	Internal Revenue Service
IRS CI	IRS Criminal Investigation Division
ISP	Internet service Provider
IT	Information technology
ITAC	Identity Theft Assistance Centre
ITRC	Identity Theft Resource Centre
NCIC	National Crime Information Centre (FBI)
NCIJTF	National Cyber Investigative Task Force
NDAA	National District Attorneys Association
NYSE	New York Stock Exchange
OJP	Office of Justice Programs (DOJ)
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OVC	Office for Victims of Crime (DOJ)
PCI	Payment Card Industry
PII	Personally identifiable information
PIN	Personal Identification Number
PRC	Privacy Rights Clearing House
RELEAF	Operation Retailers and Law Enforcement Against Fraud
SAR	Suspicious Activity Report
SAUSA	Special Assistant United States Attorney
SBA	Small Business Association
SEC	Securities and Exchange Commission
SSA	Social Security Administration
SSN	Social Security number
SSA OIG	Social Security Administration Office of the Inspector General**USA**
PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001(Pub. L. No. 107-56)
USPIS	United States Postal Inspection Service
USSS	United States Secret Service
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VOCA	Victims of Crime Act

CHAPTER 1: Introduction

Identity theft, a type of crime that has significantly come to the attention of law enforcement in the last ten years, has rapidly advanced both in volume and kind—and continues to do so. Not only has the amount of identity theft increased, but the scope and extent of the crime has expanded (Kanable, 2009; Piquero et. al., 2011; FinCEN, 2009; Langton, 2011). Until recently, identity theft most often was rooted in street crime, involving the theft of a wallet, credit card or debit card, and the illegal use of this specific item in a manner limited to the format. The crime of identity theft is going through a double process of both dematerialization, with data itself now taking precedence over what particular format it may be originally accessed as leading to a more generalized focus of identity thieves on all kinds of personal data. Moreover, identity theft is quickly moving from offline situations to the online world of the Internet, where the possibilities for identity theft are myriad, and growing more widespread and dangerous every day. Finally, as the criminal element; such as gangs and organized crime become aware of the endless possibilities that stolen identities has a marketable value, the larger the problem becomes for law enforcement. A simple theft may spiral to a chain reaction of other crimes. Therefore, the old days of law enforcement dealing with identity theft by apprehending a pick pocket or dumpster diver, now, more often than not, the criminal has, exploited the theft in surreptitious ways, by passing on the stolen data to other members of his/her organisation who will in turn convert the stolen identity into fake credit cards, and buying illegal goods, often shipping these stolen goods overseas, or selling them (Bronk, 2008; Giles, 2010). The opportunities provided by such chain-reaction exploitation have brought organised crime into identity fraud, acting as another accelerator of the scope and scale of the crime and the amounts of money stolen. For law

enforcement, all of these dynamic, accelerating forces create a type of what is termed a new crime, that is, a crime that law enforcement is still trying to understand, spiralling out of control. For this reason, a gap has opened up between the frontier of identity theft crime, and the ability of law enforcement to prevent, detect, arrest and prosecute identity thieves. This in turn has motivated still more offenders, who may have been previously involved in other kinds of theft, to move into identity theft, as they see that not only are the rewards potentially great, but that there is, at present, little likelihood of their being arrested or prosecuted, and, even should that befall them, the fact that criminal justice culture does not yet take identity theft seriously, conviction will lead to relatively light sentences in comparison with other crimes.

The current programs and systems being put in place to prevent or prosecute identity theft all appear to harbour weaknesses, preventing them from having optimal deterrent effects. The United States legislative response to date has been limited to seeking to define identity theft as a crime, and providing statutes to respond to all aspects of the crime, control the amount of personal data required to conduct business (Coats, 2008), with so-called privacy laws, and to force companies to enact data breach notification laws (Burdon, 2011). This focus has established the framework for company response to identity theft as well, which has been, thus far, to write off reimbursement as part of the cost of doing business, and pass red flag rules, which involve both training employees to detect red flags that might indicate an identity breach, and provide for a protocol that gives form to efforts to respond to breaches. Companies have also fixated on having their information management departments devise technical solutions to identity or prevent theft incidence, in effect engaging in an arms race against hackers and other identity thieves. Some critics have found that these laws are insufficient to fully address the scope, extent and seriousness of identity theft, and all uniformly fail to present any considerable

deterrence to a criminal engaged in identity theft (O'Rourke, 2005; Gellman, 2009; Leibowitz, 2012).

Company-based prevention, red flag rules, and attempts to wage a kind of technological warfare against cyber criminals, being unlikely to turn around the negative dynamic of escalating identity theft, indicate that it is time that law enforcement and criminal justice as a culture respond to identity theft in a more effective, holistic, system-wide, theoretically-grounded way, to develop models of prevention, apprehension, prosecution and conviction. To that end, this study explores the potential utility of a situational crime prevention paradigm model called the routine activities theory model as it might be applied to identity theft and fraud. Though developed over 50 years ago, routine activities theory is only partly applied in everyday police practice. Routine activities theory (RAT) constitutes a description of the social situation that enables the commission of a crime. According to RAT, a crime requires three components all coming together at once in a particular time or place: motivated offenders, suitable targets and the absence of capable guardians. That is, a criminal does not commit a crime because he or she is inherently psychopathic or simply a criminal type (a notion still espoused as an explanatory model for criminality in the popular press, but generally dismissed by law enforcement), as that state does not in itself lead to the commission of a crime. A crime occurs when the offender is motivated by the perceived value, visibility, accessibility or inertia of the object of interest, the suitability of the target or victim, involving, according to RAT, the victim engaging in predictable, routine behaviours that nonetheless, due to some carelessness, qualifies by the above criteria to attract an offender, and, finally, the absence of both social and law enforcement guardianship, that is, the absence of people, including bystanders, pedestrian traffic, and, also, police officers. When a target of value is viewed as easy to obtain and a victim behaving in a way that creates an

opportunity for its theft, in the absence of any oversight, either social or police-oriented, a crime will occur. By contrast, any preventive effort undertaken to reduce the motivation of the offender, the suitability of the target or the absence of guardianship, will prevent the opportunity for a crime to be viable.

The fact that the criminogenic circumstances involving most identity theft involves an offender motivated by the lure of quick, easy money from stolen identity, targets whose carelessness in protecting their personal information creates an opportunity for theft, and almost complete absence of any threat of being either apprehended or prosecuted with any deterrent severity, means that RAT could be applied effectively to identity theft as a more holistic model informing a more coherent law enforcement response, possibly even reducing the current upward trend in the rate of identity theft both absolutely and relative to other crimes. For this reason, this study sought to apply the routine activities theory to the problems of identity theft to determine if it was applicable in a preventive way to reduce identity theft. To explore this potential for application fully, all of the stakeholders enumerated by RAT as participating in a crime situation- an offender, a victim, and a member of the community or a member of a police department-were interviewed. This study interviewed identity theft offenders, identity theft victims and a number of stakeholders on the guardianship side of the equation, from investigators specializing in identity theft, to police department officials, to representatives of credit card companies. By this method, it is believed that a model can be presented to law enforcement, its potential effectiveness demonstrated, which might motivate law enforcement and the criminal justice system to take the crime of identity theft more seriously, and to conceptualize the crime as it is, a contagious, viral, exponentially-growing crime wave that at present, unchecked, still promises to

deeply compromise the efficacy and vitality of a new commercial and civil world built on the exchange of personal information.

(a) Background of the Study

The background to this study lies in the fact that, to date, the primary responses to identity theft in the United States, from the legislative and corporate stakeholders involved, have failed to stem the rising tide of identity theft. If the laws passed and the regulations put in place thus far had been effective in stemming the incidence of identity theft, increased response by law enforcement would not be necessary. Up to now, in fact, law enforcement has generally viewed identity theft as a lesser crime which can be managed by legislative and corporate response, not requiring an investment in manpower and initiative. Only the fact that the legislative and corporate responses to identity theft have not resulted in reduction of identity theft crime, has prompted this study, and a recommendation that law enforcement may have at its disposal models of criminality that might be more effective in framing an effective anti-identity theft effort.

The primary response to identity theft in the United States has come from legislation, and most of these laws have taken one of two forms, either they have struggled to define the nature of identity theft, and what constitutes identity theft, with these laws having to be frequently amended to account for ever-evolving novel ways of committing identity theft, or they have mandated a protocol of actions that must be undertaken should a breach in security of a firm, or the compromising of the privacy of client data be detected, mainly with the intention of outlining the accountability and responsibility of companies making use of personal data.

With regard to the first kind of law, identifying identity theft, these appear to be enmeshed in a game of catch-up, as the nature of identity theft or fraud continues to morph into new forms, all but out-running the ability of laws defining the crime to keep up. With regard to the second type of law, breach notification laws, some of these laws have been found, empirically, to reduce identity theft, in certain circumstances (Burdon, 2011). By contrast, some critics have found that breach notification laws have only limited effectiveness, for reasons likely linked to the very nature of the legislation (Stevens, 2012). For one thing, critics point out that when a breach notification law is imposed upon a company, it generally has the unwanted side-effect of highlighting the inadequacy of the corporation's current response to identity theft. Second, most of these laws are cosily drafted in consultation with corporations and thus in general, according to critics, are created with too much consideration given to the compliance cost burdens imposed by the laws on corporations, and too little attention to devising a comprehensive information privacy framework that would truly protect the consumer (Burdon, 2011). In a criticism to be heard throughout the critique of the current legislative paradigm in response to identity theft, it has also been noted that these laws to date are too specific and instrumental in nature, meaning that they are focused on the specific types of information being regulated, and the specific format-based possibilities of breach, and not on the wider social dimension of personal data sharing which forms the broader context of most personal data use today. Burdon (2011) also found that most of these laws are based on the control theory of privacy which sees privacy as an individual's choice to disclose personal information, a theoretical basis which limits the accountability of the corporation making use of the data to only notify the consumer of a breach then leave it to the consumer to make the decision about what to do. The problem is that this construction of the law leads to weak corporate safeguards, and also creates a barrier to

compliance insofar as the corporation might be reluctant to advertise a breach for fear of losing a customer. All of these laws have also, in their implementation, been criticized as sporadic and reactive, all involving actions taken after the security breach has also occurred. Most of the laws also have a one-size-fits-all quality, meaning that they often fail to take the particular circumstances of breaches into proper consideration. The weakness of the laws is exacerbated by the fact that there is no single government agency in the United States overseeing identity theft, to ensure corporate compliance with breach notification laws.

Coats (2008) also pointed out that most of these laws take the form of placing restrictions on specific types and formats of personal data that cannot be divulged, but end up leaving many loopholes easily circumvented by identity thieves behind. Coats (2008) also pointed out that most of the laws rely on their power to shut down access to certain parties to personal data according to the Freedom of Information Act, and no identity theft criminals ever access personal data in this way. As a result, this kind of law only makes it more difficult for the consumer or the company to access personal data, while having no impact whatsoever on identity theft. Nor do the laws have anything to say about the new routine practice of companies to mine personal data for leads to possible new purchases, a process which itself often leaves consumers open to identity theft. As companies collect data, tracing personal Internet activity based on such data and then making recommendations of other purchases, or managing marketing, online identity thieves routinely embed spyware in this process, and so exploit not personal data use but corporate use of one's personal data. The fact that many of the more aggressive forms of Internet marketing are not that different from spyware also blurs the boundaries between legality and criminality on the Internet, disarming legal response. The sheer volume of the data mined, and utilized by corporations, and the still greater volume of spyware generated to seek to be

embedded in that data, makes any current law seeking to prevent personal data loss by simplistic breach notification laws almost obsolete. The fact that, due to the nature of federal prosecution, some laws are utilized in ways not intended by their makers, with the Identity Theft Penalty Enhancement Act, for example, being primarily used in the context of immigration law, again disables the law (Glithero, 2009). Overall, then, in the background of this study lies the failure up to now of the legislature or statutory response to have significant effect on stemming identity theft.

The second front of response to identity theft is generated by private corporations. Companies currently seek to address identity theft in three different ways-a laissez-faire approach, a preventive approach and an embattled approach. In terms of the laissez-faire approach, many corporations take hands off posture towards identity theft. This means that the volume of identity theft has not quite yet become so grave that it has posed any significant challenges to the profits of corporations. As a result, identity theft is viewed by too many executives as an unfortunate cost of doing business, especially on the Internet, with the losses not yet having eaten into the tremendous profits being generated by online commerce. As a result, a complacent contentment with current, ineffective laws and regulations prevails, viewing identity theft as a cost of doing business (Bose & Leung, 2009).

The second company response to identity theft originates in legislation but is classified as a company response as the laws involved leave it up to the company to enforce the regulations. The Identity Theft Red Flags Rule, passed in 2008, required by law all companies who make use of credit card data to implement a written identity theft program and put in place a training program which would teach all staff how to detect signs of identity theft as indicated by so-called red flags (Bose & Leung, 2009). The red flags program mandated training and put in place a

series of response and notification procedures that a company must activate upon suspicion of a breach. Simply the fact that after the passage of the law its enforcement date had to be delayed in order to give companies adequate time to draw up such programs and policies, and the fact that a number of industries protested and won appeals that exempted them from having to draw up red flags policy, itself indicated the weakness of the law (DVM, 2009). Lee (2009) pointed out many cases in which companies in different industries faced great challenges in drawing up adequate red flag rules, involving an enormous amount of work, almost to the extent of writing legislation for them, often resulting in partially successful codes and regulations. As a result of leaving the authorship of the red flag rules up to companies, most made do with simplistic lists of red flags that appeared to Lee (2009) to have more to do with the company meeting minimum compliance requirements than fully protecting consumers making use of personal data when doing business with that corporation. McMillion (2009) noted that law firms were able to lobby themselves out of the law based on the argument that they were generally too small to undertake such an effort. Kunick & Postner (2011) also argued that it was highly unlikely that many other kinds of companies had sufficient in-house skill sets to develop thorough red flag rules. The end result of red flag rules implementation problems is that a template of red flags has emerged as standard practice, and it constitutes quite a basic notion of the dangers of identity theft. The fact that corporations often are lax in their handling of personal customer data caused Listerman & Romesberg (2009) to argue that what is required is not a list of rules, but a culture of security created through a routine provision of identity theft awareness and protection seminars, full leadership support of anti-identity theft efforts and full ownership of the program. Red flags are limited in scope to private industry and not to government agencies. This strikes McKee & McKee (2011) as a mockery of the law. Each year, the federal government has tried to address

the issue, resulting in an increase of criminal activity, enforcement cost and additional losses to the American public. Finally, Clapper (2010) pointed out, as with other laws noted above, that the technical and functional approach taken by the red flag rules, itemizing specific warning signs in specific media, fails to take into consideration the wider dimensions of identity fraud and the ever-growing number of ways in which identity thieves can get at personal data.

In sum, most aspects of the current law enforcement regime designed to prevent identity theft, consisting of laws that define identity theft, breach notification laws, red flags rule laws and company compliance laws, appear to the federal regulators to be inadequate in terms of addressing the growing scope and expanding dimension of identity theft. Identity theft has increased exponentially as a crime. As a result, it continues to morph into new forms that repeatedly outstrip efforts to define and expand law and that the speed and expanding scope of the crime, especially as it moves from offline to online criminal opportunities, is in danger of making breach notification and red flags rules as the primary instruments of a reactive paradigm against identity theft obsolete.

(I) Technical Response to Identity Theft

Business itself seems to have experienced a dawning awareness of these limitations, and perhaps motivated by projections that in the future identity theft will, or is in the process of becoming a problem that will necessitate a response, have begun to engage more often in a second front of defence, or even offence, against identity theft, by sponsoring the development of ever more complicated and sophisticated technical responses to the crime. Many large corporations have set their IT departments against identity theft, leading to the devising of

numerous new strategies. These efforts are framed by a technical paradigm, which is premised on the notion that, especially on the Internet, identity theft is enabled by the advancing technical skills of hackers and phishers, and others, and that the best response is—better technology. Criticism that preventive or responsive technology has fallen behind the sophistication of hackers has generated this approach. The rhetoric overarching this discourse, including futuristic scenarios of cyber war, brings military, security and even law enforcement into the technical scenario for defeating internet-based identity theft. This approach is primarily focused on large scale investments in developing sophisticated information weapons. The results will be observed when society sees a return on that investment benefiting the economy, while attacking massive hacking and phishing identity theft activity on the internet. This will be a daunting task, demonstrating almost horrifying escalations in the number of spyware, malware, phishing sites, spoof sites, other schemes and hacking efforts. It is also true that this response has produced a number of impressive victories. At the same time, defeat is common. Simply the rhetoric of the effort, positing victory or defeat in a game of confrontation described as a war, underscored the difficulties involved in the sustainability of this approach. By taking this approach, corporations embroil themselves in virtual combat, which sets off a kind of arms race, one response being met by another, then the identity thieves devising still another response. It is an unending and unintentionally escalating dynamic that cannot in the long run lead to a genuine solution. Otto (2009) pointed out that the complexity of the opportunities for identity theft in various aspects of the design, development and deployment stages of software production makes it unlikely that a purely technical approach to combating identity theft will ever be successful. On the basis of his analysis, Otto (2009) argued that establishing standards and enforcing compliance to them was likely to be the best way to prevent identity theft. Nonetheless, a host of technical solutions are

rolled out seeking to combat hackers and phishers. These include biometric devices (Al Harby, et al. 2010), which would be at the centrepiece of new security regimes at banks and other sites where identity is stolen, and creating better accountability in internet systems through management of trust. All of these mandated devices would attack spam and other avenues of theft (Aggarwal, et al. 2010). In addition, simply reframing the defence of the internet and its viability, by making policy that manages "intermestic security" wholesale attacks (as those launched by botnets en masse against computer systems) can be stopped (Bronk, 2008). This latter approach would involve reconceptualising the concept of national security in the context of a globalized world of intense interactiveness where such security is breaking down and replacing it with a new transnational policy framework that regulated the internet from a global perspective. While ultimately, this framework would create mechanisms by which local and global law enforcement agencies could work together to combat identity theft, and, in doing so, such an intermestic framework would undo the jurisdictional constraints that at present make law enforcement of identity theft so difficult, Bronk (2008) conceded that such a transnational policy framework has yet to take shape.

In lieu of these frameworks emerging, more holistic frameworks which already exist must be considered as resources for improving identity theft detection and prosecution. The cooperation of legislative, corporate and law enforcement in combating identity theft would make this kind of framework operable. My research will explore the necessary cooperation that is needed. However, the legal frameworks adopted by legislators, and the notification and technical solutions offered by corporate protection, do not yet seem capable of reconceptualising identity theft in a holistic way. This leaves criminological models utilized by law enforcement as a body of work that is exploitable for this purpose. Indeed, a good deal of research has argued

that these approaches offer more promise for preventing and combating identity theft, than frameworks derived from other fields. Already, examples of more holistic approaches to combating identity theft, involving technology and law enforcement, have been documented. Greenwood (2009), for example, described a scenario where police embedded Comptrace technology in laptops so that, if stolen, their location was able to be traced and the criminal apprehended. However, even with this tracking type approach falls short of totalling addressing the needs of law enforcement.

Thus far, law enforcement offers situational crime prevention theory and models as a holistic approach to combating identity theft (Tillyer & Kennedy, 2008). By and large situational crime prevention methods expand the focus of the crime from the crime itself to the victims and targets of the crime. The purpose of this approach is to study how potential victims behave in ways that leave them open to criminal attack. The broader purpose of a situational crime prevention analysis and awareness program would be to educate victims to not engage in activities or behaviours that have been found, statistically, to leave them open for crime. Routine activities theory presents a model of a crime consisting of a motivated offender, a suitable target and the absence of guardianship. The crime only occurs if all three elements, in optimal form, come together in time and place to create an opportunity for a criminal. Optimal form means that the offender motivation is high due to the ease of the target, its value measured against effort, and the likelihood of his or her encountering prohibitive guardianship or deterrence. This approach is situational as it focuses on the dynamic of criminogenic situations, as opposed to fixating on, for example, the mental state or morality of the criminal. It is also preventive as, according to the theory, the likelihood of the crime can be greatly reduced if the optimal imbalances in these three factors can be rearranged against the offender, thus reducing his or her

motivation to commit the crime. That is, if the offender motivation is reduced, through various means, the suitability of target reduced, also through various approaches, and the presence of guardianship, which can include the threat of arrest, prosecution and a heavy penalty, then crime, will decline.

A number of case studies have been published demonstrating the effectiveness of this holistic method in reducing incidence of crime of various types. Cromwell et al. (2008), for example, demonstrated that an SCP approach was able to reduce incidence of crime in libraries by having both the library and its users alter their policy or behaviour in various ways. Mensch & Wilkie (2011) described efforts by colleges to reduce identity theft on campus and online from campus by increasing student awareness of the dimensions of the crime as a way to reduce their victimization.

(ii) Statement of the Problem

The problem to be addressed in this study is that current means of combating identity theft appear to be failing, as indicated by the ever-escalating spirals of identity theft, its apparently contagious character at present, spreading into all kinds of criminal activity, and the failure thus far of the criminal justice system to gain a measure of control over the crime. The core of the problem appears to be that the most popular approaches developed to combat identity theft, a legislative response then left to corporations to carry out, is a reactive response to the crime, involving merely alerting a victim to suspicious activity on their account, by means of red flags, or notifying them of a breach of the security of their personal data, under a breach notification law. Though corporations in particular seem enchanted by finding a technological

silver bullet to solve the identity theft, it appears to be a consensus in research that this 'arms race' approach will always lag behind the capacity of online identity thieves to develop ever newer and more complicated ways to steal identities. Adding to the overall problem is the problem that law enforcement at present seems to be complacent about the crime, under appreciates its seriousness, downplays it compared to other violent crimes, and does not take it seriously, meaning that judges also fail to hand out sentences for this crime that would have a deterrent effect. The involvement of law enforcement in the current regime of identity theft crime-fighting, moreover, usually becoming involved in breach notification, is far from best practice, usually counterproductive and very often ineffective. Indeed, law enforcement in general at present espouses the view that there is nothing that can be done by them to combat identity theft. This problem is made even more immediate to surprised victims when law enforcement informs them that, due to the fact that the crime committed on their stolen credit card number happened overseas, that this is out of their jurisdiction and there is nothing that can be done. Clearly, the failure of law enforcement, as well as other arms of the current paradigmatic response to identity theft, represents a serious problem that must be resolved. It is the goal of this study to contribute to improving law enforcement understanding of the seriousness of identity theft and ways to combat it through prevention by proposing that the situational crime prevention routine activities theory approach to crime be applied to identity theft to provide a battery of preventive, reactive and deterrent response to the crime.

(iii) Purpose of the Study

The purpose of this study is to gain a sense of the perceptions of key stakeholders involved in the crime of identity theft. The stakeholders chosen for interview are based on the

routine activities theory model of a crime entailing the coming together in time and place of a motivated offender, a suitable target or victim, and the absence or presence of a guardian, or the police and the police department. To fulfil these dimensions, the purpose of this study was to reach conclusions by interviewing investigator specialists in identity theft including law enforcement officials and various stakeholders. The objective was to explore how offenders view identity theft as well as, to gain a sense of their perception of the RAT factors which contributed to the crime. It is the larger purpose of this study to analyse all stakeholder responses with an eye toward providing recommendations, based on routine activities theory, as to how each stakeholders views could be altered in ways that would reduce incidence of identity theft. For police personnel, this would involve changing perceptions so that practice and prosecution is more diligent, for offenders, this would involve changing perceptions of the attractiveness of the crime, and for victims, this would involve changing perceptions so that they not only altered behaviour that may have made themselves available to the crime, but also reduce the confusion and shock that results from being victimized, so that the crime of identity theft, with a broader knowledge about it, is demystified.

(iv)Theoretical Framework

The theoretical framework of this study is the situational crime prevention paradigm, with a focus on routine activities theory, both well-known criminological theories which have been utilized extensively by law enforcement practice to reduce crime through a holistic approach including both prevention and prosecution. Situational crime theory argues that criminogenic circumstances and opportunities are more likely the cause of crime than the personality of the criminal, the attention of the police to quality of life crimes (broken windows

theory) or the concentration of crime of one type in one place (hot spots theory), though elements of these theories feed situational crime efforts. Situational crime theory argues, that is, that it is the situation, and its variable dynamics, that leads to crime being committed, and that if the situation is altered then the crime can be prevented. According to routine activities theory, the leading cause of crime is the routine, everyday activities that people undertake in ways that leave them open to exploitation by criminals. While routine activities theory is not popular, as some political lobbies believe that it serves to blame the victim, or sends an unhealthy, paranoid or false message to the public (for example, if a police force, upon investigation, found that a person suspected of molesting women found that his modus operandi consisted entirely of attacking women wearing a certain type of short dress, for the police to caution women against wear this kind of dress would clearly be interpreted by women as blaming the victim). However, routine activities theory has repeatedly documented, in various types of crime, that people routinely engage in daily activities that leave them open to be victimized. Therefore, the first step to be taken in preventing crime is to take the opportunity created by that routine activity away from the criminal (Boetig, 2006).

According to the theory, crime is prevented by "systematically manipulating or managing the immediate environment in as permanent a way possible, with the purpose of reducing opportunities for crime as perceived by a wide range of offenders (Tilley & Kennedy, 2008, p. 76). On the other hand, a Smartphone is ideal, it is used carelessly by millions of consumers, they are everywhere, they are lightweight, they can be lifted in a split second of consumer carelessness, the criminal can remove himself from the scene quickly, there is little chance of finding it and they are worth, for the moment, a good pay-off amount to a fence. Guardianship is present or absent as a result of time of day or night, type of street, domestic or commercial, and

the presence of absence of other people, such as group of friends, a crowd, shopkeepers or police (Fell, 2006). These are all termed controllers in the RAT scenario, but additional theory has also posited that super controllers play a part in determining how seriously criminals take the threat of controllers. For example, increasing the penalties for a certain type of crime may make police presence into a much more formidable factor in strengthening the guardianship of the situation, whereas police presence un-backed up by strong laws and certainty of prosecution would seem to disarm them, in the criminal's mind. In this way, a situation is conceptualized by routine activities theory as having many variables or moving parts, manipulation of which can change the equation in terms of the likelihood of a crime occurring. That is, if the situation entailed a highly motivated offender, an imminently suitable target and the absence of guardianship, it is likely that a crime will occur. If, however, a situation entailed an unmotivated offender, a target whose behaviour or activities makes them unsuitable for attack, and the presence of guardianship, it is unlikely that a crime would occur. If, after a proactive analysis of the situations occasioning the occurrence of any particular type of crime, the police determine that the former situation exists, a primary part of the routine activities theory-based work that they have to do is to change behaviours in such a way as to convert that situation into the latter type, where crime is unlikely to occur. Police are likely to do this by interfering with all of the criminogenic aspects of the situation. Routine activities activity has gained a measure of credibility by being shown to be borne out by application in a number of different criminal scenarios. RAT has been found, generally, to be an effective approach to preventing crime.

Finally, one of the most promising aspects of routine activities theory is that, having already adapted it to many different criminal situations the theory is imminently expandable to application to any new situation that comes along. Every time some dynamic in society, whether

urban or suburban, based on population movements, the transformation of neighbourhoods or the development of new markets, RAT can be applied. RAT can likewise be applied to that new platform of modern commercial life, the internet, which, in the last two decades has evolved from a network for the sharing of scholarly discourse and the sending of emails, to online shopping, to social media, at every stage in the evolution of which new situations in which crime could occur were created (Boating, 2006). RAT also applies to the Internet because just as on city streets or in daily life offline, consumers engage in routine activities that either protect their safety from, for example, identity theft, or act in ways that expose them to the likelihood of being victimized. Particularly as engaging in commerce on the internet necessitates entering in credit card numbers and passwords, not to mention security questions, the fact that this information is required for a transaction to occur, opens up the internet to new opportunities of theft. For this reason, RAT applies to online situations as well as offline situations: the goal is to address those aspects of offender motivation, target suitability and presence or absence of guardianship that might make a situation safe or insecure. It is because of its flexibility in application to all manner of criminal situations that routine activities theory was thought to be an ideal framework for tracing all kinds of identity theft crime from offline to online situations.

(v) Research Questions

The following research questions guide this study:

1. What is identity theft?

2. How did identity theft evolve as technology and cyberspace became readily available to the general public?

3. Who are the identity thieves, what methods do they use in committing identity theft and how did they acquire the skills that are needed to commit identity theft?

4. Who are the victims of identity theft, how do they expose themselves to the identity theft and how has identity theft altered their activities and behaviour?

5. What have been the strategies of the executive and the legislative branches of the United States government, including law enforcement, to address identity theft and what challenges do they face in their effort to detect, investigate and combat identity theft?

Routine activities theory was utilized to frame an instrument to guide interviews by asking, of different stakeholders, specific questions about offender motivation, suitability of target or presence or absence of guardianship. Offenders were questioned regarding what motivates them to commit a crime, how they committed a crime and what made it possible for them to do, both on the street and online. Victims were questioned about the extent to which their behaviour created opportunity for crime both on the street and online, and if they have taken onto themselves guardian roles by changing their behaviour to a more defensive stance. Stakeholders in law enforcement were questioned as to the degree of their guardianship both offline and online in identity theft situations, as well as battery of super controller questions involving how much focus their department, police culture and the criminal justice system as a whole puts pressure on them to combat identity theft, or even takes the crime seriously.

(vi) Nature of the Study

The nature of the study is grounded in the fact that the researcher is an experienced investigator specializing in identity theft working in the Manhattan District Attorney's Office, in

New York City. The experience of investigating identity theft, encounters with the limits of current prevention, the awareness of the growing and accelerating dimension of the crime, the fact that individual physical-object based theft is quickly being supplanted by internet-based theft, the scope of the crime accelerated by the increased participation of organised crime in it, all have motivated the researcher to explore the crime and discover ways to improve law enforcement response. Because rooted in experience, the nature of the study is primarily ethnographic (see methodology), which means that many interviews were conducted in circumstances of constraint adjunct to the everyday practice of the researchers in law enforcement (though a leave was taken and at no time, when interviewing subjects, were they not notified that the interview was confidential and restricted to the study). The interviews, with 25 offenders, 25 victims and 25 investigators, law enforcement officials and other stakeholders were collected over the course of several years. The interviews were coded to account for the ethnographic factors that might compromise validity. The results of the interviews were then analysed individually and summarily in order to reach conclusions about the current state of perception of these stakeholders, relevant to their appraisal of the motivation, suitability and guardianship factors that either enable or prevent identity theft from occurring. Implications for future practice were drawn up based on the results of this analysis.

(vii) Significance of the Study

The significance of the study lies in the fact that identity theft, due to the rise of the internet as a major location of commercial transaction, as well as the emergence of social media, and due to the increased involvement of organised crime on a global level in the crime, is at

present no longer being adequately prevented by the current paradigm designed to combat it. A reactive approach must be replaced by a more holistic approach, also involving prevention and deterrence. Thus, current practice in law enforcement is based on a single legislative-corporate paradigm which is focused on reactive notification after the fact. Other paradigms must be explored to find a better way to gain some control over the identity theft epidemic. Criminological theory, including situational crime prevention, and routine activities theory, has been developed to assist law enforcement to improve its practice in combating all manner of crime. At present, however, application of this holistic approach to identity theft is lacking, and as a result in the current paradigm police often are left to espouse a laissez-faire or nothing-can-be-done attitude toward the crime. Therefore, any effort undertaken in research to attempt to alter the status quo is significant, insofar as it offers potential for an approach that will curtail the ever-escalating nature of this crime.

Conclusion

This study explores the problem of the ever escalating incidence of identity theft in scope and scale, evolving into identity fraud undertaken by organised crime for the purpose of creating all the false documents necessary to create a false identity for illegal persons. The study is particularly focused on the extent to which the development of the internet, and online shopping and social media, have contributed a host of new situations in which identity theft can occur. In order to examine the problem, and offer some preventive solutions to the problem, and in lieu of the weaknesses in the current paradigm utilizing red flag rules, breach notification laws, and characterized by lack of law enforcement prioritization and punishment for this type of crime, this study enlists the criminological situational crime prevention and rational choice based

routine activities theory which argues that situations engender crime, and not innate characteristics in persons involved. RAT is utilized to frame a battery of questions asked of offender identity thieves, victims of identity theft, as well as stakeholders in law enforcement, in order to determine their perceptions on why identity theft as a crime continues to grow. At present, it appears, according to routine activities theory, that the situations in which the crime takes place, both offline and online, are characterized by high offender motivation (and only getting higher because the higher pay-off in more sophisticated uses of stolen personal data), high target suitability (characterized by careless consumer behaviour with regard to personal data both offline and online) and low guardianship (characterized by relative lack of concern about or inability to respond effectively to identity theft). It is the hypothesis of this study that if the situation of identity theft could be changed through a combination of preventive, prosecution and deterrent action to one characterized by low offender motivation, low target suitability and high presence of guardianship, law enforcement could contribute much to stemming the rising tide and even epidemic and viral nature of identity theft as it sweeps through the criminal world and everyday American and global commercial life.

CHAPTER 2: Literature Review

(a) Introduction

This literature review was drawn from a search of the following EBSCO databases**:** Academic Search Premier and MasterFILE Premier**,** utilizing keywords such as identity theft, identity fraud, phishing and dumpster diving. The results of the review will be compared to the public record of recent legislation regarding identity fraud, police records and interviews with investigators specializing in identity theft in various police departments, police officials, and impacted stakeholders such as CEO's of credit card companies, identity theft offenders and identity theft victims. The review establishes that identity theft, a relatively new crime, has soared in recent years, with the internet becoming, either ultimately or exclusively, the primary site and most important enabler of this new kind of crime. While credit card fraud and laptop theft are occasions for a considerable amount of identity theft, it is also true that the quick development of ever more sophisticated hacking and phishing techniques by hackers online, combined with exponential growth in online shopping and use of social networking sites, has relocated the focus of identity theft to the internet (Bronk, 2008; Giles, 2010). Therefore, the review focuses attention not only on how personal data is originally stolen but also on the extent and type of identity fraud which is committed by way of the Internet. When it comes to the response by law enforcement to identity theft crime, while it would seem that laptop or credit card theft could be responded to in ways that fit into pre-existing paradigms for combating theft generally, the novelty of internet crime has placed law enforcement in a defensive position (Burdon, 2011; Coats, 2008; Glithero, 2009; Winn, 2010). Moreover, the evolution of the internet and crime on the internet has resulted in the emergence of a paradigm of information

specialists who believe that the ever more sophisticated tools used for identity theft can only be met by technical development of more tools to combat the crime, in essence, engaging in a kind of technological warfare or arms race on the world wide web. The review finds that while the technological response paradigm is strong, government response has been less robust. Government response, through legislation, appears to be split over how to respond to identity theft, with some calling for the creation of rules that companies must, by law, enforce themselves, so-called red flag rules, and others arguing that these rules are too easily superseded by advances in crime and that more general field-wide standards are the best approach (Bose & Leung, 2009). The self-policing and employee-awareness focus of the red flag rule paradigm in particular, however, has much in common, in its approach to crime, to preventive models of crime response in policing. Indeed, the review proceeds to consider how, if most of the focus in identity theft prevention is on red flag rules, industry standards or improved technological response, exactly law enforcement can help combat identity theft.

Using the theoretical model of situational crime prevention, which includes the routine activities theory of crime reduction, the review demonstrates the efficacy of both models in reducing crime, especially theft (Boetig, 2006; Groff, 2008; Miethe & Sousa, 2010). By outlining the principles of the situational crime prevention model, moreover, the similarity between its methods and the language used by proponents of red flag rules, with the focus on consumer awareness training and reduction of the opportunity for crime, is made clear. The review finally turns to case studies of law enforcement efforts to respond to identity theft (Mensch & Wilkie, 2011; Ramsey & Venkatesan, 2010; Reyns, 2010). Though at present this remains an understudied area, a few researchers have, in fact, explicitly done some theoretical model-building by applying the situational crime prevention and routine activities theory

framework specifically to identity theft, and also to identity theft online. Here, as in other paradigms, consumer awareness training, removing opportunities for crime and increasing the guardianship role of either controllers or super controllers (which would encompass industry standards as well as legislative response) would reduce crime. To help all stakeholders embrace a culture-based preventive approach to reducing identity theft, as opposed to getting involved in what at times seems like a hopeless arms race against technological-based theft, law enforcement therefore has a strong advisory, consultant and even investigatory role in preventing identity theft.

In sum, this literature review will provide an overview of research literature to date focusing on the research questions which are the focus of the study. First, the review will examine efforts to identify identity theft, and the dimension of its incidence in recent years through statistics and analysis of the trends and patterns of identity theft crime. Second, the review will address the issue of how the growth of identity theft has been facilitated by technology and the expansion of cyberspace, bringing identity theft criminals in more routine opportunistic contact with the general public. Third, the identity of identity thieves, fraudsters or scammers will be reviewed, as will the means by which these individuals were able to acquire the skills needed to commit identity theft. Fourth, the review will examine research concerning the various mechanisms employed by fraudulent individuals in order to commit their crimes, with attention paid as well to offender motivation, the organizational qualities of the work, and the degree to which identity theft supports or is supported by other criminal activity. In this study, the mechanisms will be limited to fraudulent use of credit cards, debit cards, bank accounts, personal information for obtaining loans, with regard to criminals; as well as the nature of the occurrence of the actions (separately or concurrently), the quickness of discovery, how the victim became aware of the theft, the total dollar amount, how they responded (closure of

accounts), and other negative consequences of the crime. Finally, the review will study the impact of the criminal justice system in the United States on the volume and rate of identity theft, what the branches of government, as well as the criminal justice system, have done to address identity theft and the challenges the system continues to face in its efforts to stem the rising tide of identity theft. All of these concerns are directly related to the research questions underlying this research project, by way of testing the efficacy of applying routine activities theory to the prevention of identity theft today.

(i) Statistics, Trends and Patterns of Identity Theft at Present

According to a recent survey, in February, 2011, there were 8.1 million identity theft fraud victims in the U.S. with the crimes amounting to $37 billion in losses. While out-of-pocket losses to victims of identity theft remain limited, they rose from $387 per victim in 2009 to $631 per victim in 2011, an increase of 63% (Curtis, 2011). There is evidence that identity theft rates began to accelerate in about 2005 (Jefson, 2007). From 2005 to 2007, 255,565 people in the U.S. were victims of identity theft. At that time, the most prominent type of identity theft was credit card fraud. It is likely that the rapid escalation of identity theft fraud created a gap between a crime wave and law enforcement, as it would appear that, insofar as 61% of victims failed to notify police departments of the crime, victims themselves were unsure of what crime had been committed against them. In 2008, a then record-setting 275,284 complaints of identity theft were reported by the FBI Internet Crime Complaint Center (Wagner, 2009). The cost to consumers or companies of fraud has increased from $68 million per year in 2004 to $265 million per year in 2008 (Wagner, 2009). The fact that 29% of victims of identity theft are between the ages of 18 and 29 suggested to Jefson (2007) that young people may be either naïve or too idealistic about

Internet use and need to be instructed on the nature of identity theft. Indeed, Jefson (2007) argued that more consumer education on the nature, causes, ways and growth of identity theft may be required as a fundamental approach for reducing consumer exposure to the crime.

Listerman & Romesberg (2009) further broke down the profile of which types of companies are targets of identity theft. In the context of a 400% increase in identity theft between 2005 and 2008, Listerman & Romesberg (2009) found that businesses generally experienced the most incidents of theft (240), educational institutions came next (131), the military and government experienced 110 incidents, while medical settings had 97 and financial 78 breaches of security. As a result of this growth, a number of federal laws that impose penalties for the mishandling of personal information were drafted, and most laws apply to small as well as large companies. Listerman & Romesberg (2009) also found that incidents of identity theft negatively impacted company-customer relations, with one study finding that if a company reported an identity theft incident it might well expect to lose 20% of business outright, 40% of clients will have questions about their services and 5% may sue the company. Indeed, this kind of figure may in fact make companies unwilling to abide by red flag rules which mandate that incidents of theft be reported to consumers.

(ii) How did Identity Theft Evolve as Technology and Cyberspace Became Readily Available to the General Public?

Berg (2006) found that identity crime evolved quickly, once technology became involved, as technology allowed criminals to perform new and more complex forms of fraud. The theory of the three phrases of technology-enabled impacts argues that there are, online, ordinary, adaptive and new crime, with ordinary crime defined as well-known types of crimes, adaptive crime being variations on ordinary crime but with innovations added afforded by technology, and

new crimes which “are typically not well-understood and involve radically innovative use of technology to commit” (Berg, 2006, p. 10). With new crimes in particular, law enforcement struggles to understand the crime and keep up with ever newer innovations. These new crimes put law enforcement at a disadvantage while they struggle to understand the “new crime” and also to keep pace with newer innovations. One may conclude that “new crime” may also be defined by the fact that the policy lag enables this occurrence. Even though law enforcement efforts were on the cutting edge, the bureaucracy and policy developers were slow in implementing those innovations. Adding to the complexity of Internet crime is that some victims do not see themselves as such, or even know they have been victimized, often making these crimes classifiable as victimless. As a result, file sharing, downloading mp3 files and other illicit activities online are not viewed as criminal because they are victimless. Victim precipitation theory, however, argues that the victim was somehow responsible for the crime, by behaving in a way that created an opportunity for the crime, and shoring up victim behaviour has been one approach to combat Internet crime. By contrast, lifestyle exposure theory argues that contrasts in lifestyle can open persons up to criminal victimization. Finally, routine activities theory argues that “structural changes in routine activity patterns influence crime rates by affecting the convergence in time and space of three elements of direct-contact predatory crimes: motivated offenders, suitable targets and the absence of capable guardians against a violation” (Berg, 2006, p. 18). On the internet, the routine activity would be any number of habits in surfing or emailing, and the opportunity created by unsecure habits in doing so, but guardians can be provided in various ways, through access control lists or other means. Also, routine activities theory has been utilized to explain how everyday real-world crime can contribute to identity theft, in, for example, the theft of a wallet leading to the illegal use of a credit card. Occurrence of the crime

may also, according to the theory, prevent recurrence, as the victims may change their behaviour by using anti-virus software or shredding documents, or not giving out their Social Security numbers. Indeed, the primary forms of identity theft involve credit card theft and electronic banking fraud, illegal use of Social Security numbers, misuse of ATM's, all of which developed alongside of technological developments in the banking industry. The expansion of the use of various pieces of personal information over time has also contributed to criminal opportunity.

The Social Security number was first instituted in the United States in1935 to keep track of funds to be directed back at workers upon retirement, and originally intended to be only used in the Social Security Administration. In the 1960s, however, it began to be adopted as a basic unit of ID for federal employees, taxpayer identification with the IRS, Medicare, Veterans Administration admissions, and bank records. Here, too, then, online identity theft using SSNs is the result of an opportunity created by a long-term expansion of the use of the number for ID purposes, possibly undermining the original security of the number. Some 26% of ID theft entails credit card fraud, 18% unauthorized phone use, and 17% bank fraud.

(b) Moving Toward the Internet

Most of the gain in the amount of identity theft is attributable to the internet becoming the primary and increasingly dangerous site of identity theft. The proliferation of malware is getting worse, worrying experts. Information Week (2009) reported that in the first half of 2009, for example, the number of fake anti virus programs being utilized on the Internet to extract personal user information had increased by 585%. The number of so-called banking Trojans, moreover, programs that steal account information from financial sites, had increased 186% during the

same time. One commentator therefore asserted that “the Internet has never been more dangerous” (Information Week, p. 1). So prevalent is identity theft that Information Week (2009) also identified its world as “the identity theft underground,” a whole sector of the Internet where the number of malware programs designed to steal personal information has risen 600% in recent years (p. 1). The fact that a number of the newer malicious software or malware, such as the Zeus Trojan, designed to steal passwords and user names, are more sophisticated than ever, and have also challenged science information experts. Another of these programs, the URL zone Trojan has anti-forensic techniques in it that conceals that it is looting data by issuing false bank reports to users to cover the fraudulent transaction. This then would undermine the breach notification reporting approach to preventing identity theft, as the user would have little sense that they have in fact been hacked. Many criminals are also making use of the Plucky cybernetic tool kit to compromise legitimate web sites, in effect turning detection software against itself. One gang made use of the program to attract 90,000 visitors to their false site, 7.5% of which provided data and were infected, allowing them to make over $400,000 in 22 days. In 2009, moreover, 66% of all companies reported at least some infection of computers by malware, and 54% of all computers also are infected. While acknowledging that the tech industry responses to these advances are equal to the task in many ways, Information Week (2009, p.2) commented nonetheless that “no doubt there’s more to be done.” The urgent need for reform is reinforced by findings from consumer polls that 66% of U.S. adults worry frequently about the danger of identity theft, representing more concern over this issue than worry about having their car stolen or their home broken into (Saad, 2009).

(i) Malware

Some experts speculate at convergences in areas of crime leading to rise in malware on the web. For example, one expert argued that "the global economic downturn and the thriving black market for credit and debit card numbers and online account information is driving the creation of so much identity stealing malware" (Information Week, 2009, p. 1). The fact that malware can also be transmitted through Facebook and Twitter has contributed to the rise of malware on the web. One detection company reported receiving reports of new malware, ranging from viruses to Trojans, being launched at a pace of 35,000 per day. Trojan programs stealing bank information constitute 71% of that total, an increase of 51% since 2007, and strongly indicating that banks are one of the primary targets of identity theft criminals. Moreover, in addition to stealing identity by spoofing online bank sites, spoofing of PayPal, Amazon and eBay is also on the rise. Malware also appears to be generally shifting its focus from email to social media sites. Reporting on a case where Alberto Gonzalez was successfully prosecuted for hacking a corporate computer and stealing more than 130 million credit and debit card numbers, it remains questionable whether or not this kind of prosecution will be able to stem the rising tide of identity theft. Information Week (2009) expressed the notion, "whether law enforcement can keep up with the growth of the identity theft industry remains to be seen" (p. 2). Breaches of security with regard to credit card data have become particularly problematic, with Smith (2009) estimating that in the previous five years 494 million sensitive records have been compromised, and this only in publicly reported data breaches. Eight large breaches at major banks accounted for 79% of all compromised records. At the juncture of law enforcement and identity theft, then, there appears to have developed a fundamental question of the capacity of law enforcement to combat this problem in an effective way. Indeed, the research into combating identity theft

generally appeared to focus on the paradigm of a technology warfare response to identity theft (Smith, 2009).

(ii) Fake Websites and More

The major contributor, then, to the rise of identity theft as a crime is the internet (Bronk, 2008; Giles, 2010), where fraud and deception are prevalent, "impacting hundreds of thousands of internet users" (Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010, p. 435). Formerly, security attacks on the internet primarily targeted software vulnerabilities, but a new class of attacks "leverage the information asymmetry of online settings to exploit human vulnerabilities" (Abbasi et al., p. 435). Abbasi et al. (2010) in particular examined the problem of fake websites as a growing problem, finding that up to 20% of the entire World Wide Web consists of fake websites designed specifically to extract private data from users. Moreover, 70% of .biz domain pages and 35% of .us domain pages have been found to be fakes. Consumers are increasingly reporting having data stolen from fake websites with one anti-theft working group reporting that in one month they received 20,00 reports of such crimes. A significant problem is that most consumers cannot tell the difference between a real and fake website, are unaware of the existence of fake websites and fraudsters are always improving their skills in terms of undermining protections against them. Studies of why users make use of various sites also has found that insofar as the look of a site is important for establishing consumer trust and use of the site, the high-quality appearance of many fake websites entices users to enter in sensitive data. One study of consumer behaviour with regard to fake websites found that 82% of tested consumers entered in personal information to a fake website, primarily because they believed it was a real site.

By and large, there are two groups of fake websites, those targeting search engines, or web spam, and those that attack web users, with this group including both spoof and concocted sites. Spoof sites imitate existing commercial websites such as eBay, PayPal and banking sites, thus deceiving consumers to divulge sensitive personal information. Spoof sites have been reported to have been used to attack millions of internet users. By contrast, concocted websites attempt to look like legitimate commercial sites, and primarily engage in failure-to-ship fraud, that is, they elicit consumer ordering, then have nothing to ship to the consumers. Formerly, fake website detection has been the primary method used to protect consumers from these websites. Most of these systems were described by Abbasi et al. (2010) as lookup systems entailing blacklists of URLs derived from reports of fake websites for online trading communities. An Internet user can sign up with a group such as the Anti-Phishing Working Group, or a lookup system, as such the IE Phishing Filter and Mozilla Firefox's Firephish, among many others, in order to avoid using a fake website. The main problem with this approach to protection is that it is reactive, meaning that the user has most likely already been victimized by the site before they report it. Thus, blacklist prevention does not seem to work well. For that reason, proactive classification techniques have been developed to detect fake websites using a series of fraud cues such as design element of the sites. The main problem with this method is that most of these fraud cue heuristics are, in Abbasi's et al. (2010) view, simplistic and easy to circumvent. The fact that fake website detection occurs in a highly dynamic situation where as soon as fake website creators sense they are being found out they are on to creating another site makes both of these methods also ineffective in keeping up with the pace of criminal activity.

Detection of fake websites using these methods has been estimated to be below 70%, meaning that by and large these remain ineffective responses. For that reason, Abbasi et al. (2010) proposed a new fake website detection system based on statistical learning theory. This method, called the AZProtect method, does not overly rely on human reporting, and can incorporate large quantities of data on websites. Statistical learning theory is a computational learning theory that explains learning statistically, featuring such elements as the theory of consistency of learning process, the non-asymptotic theory of the rate of convergence of the learning process, the theory of controlling the generalization ability of the learning process and the theory of constructing learning machines that can execute the learning process. Without detailing the algorithmic basis for the means by which these ideas are embedded into a fake website detection system, the resulting system nonetheless provided a much richer way of detecting fake websites. Having built a model, Abbasi et al. (2010) tested it empirically in exercises to detect fake websites, using a considerably expanded fake cue set, and the underlying linear composite SVM kernel. Using more classifiers of fake websites, the study found that the method was in fact able to detect more fake websites than existing methods. As in all such studies, however, the implications for prevention of identity theft through any number of means on the Internet, including fake websites, strongly implies a paradigmatic belief by computer programmers that they can combat fraud with technological improvements in anti-fraud efforts on the Internet itself. The extent to which internet fraud prevention thus becomes a cyber battle between two opposing groups armed with highly specialized knowledge of information technology would seem to hinder law enforcement from effective participation in these efforts against identity theft.

(iii) Social Media

The spread of social media has added another layer of complications to the problem of reducing Internet-based identity theft. Giles (2010) reported on a study that found that it was easier for website owners to identify users if that user had a more active social network and social media use history. Thus, "when you sign up for a membership group on a social networking site you may be revealing more than you bargained for" (Giles, 2010, p. 1). This is because other websites can extract your name and from it gain a history of your surfing on the web, making you vulnerable to identity theft. Giles (2010) reviewed a case study in which this unauthorized use of data collected from social media sites was expedited for the purpose of committing identity theft. While social media sites have begun to add random numbers to mask addresses, to prevent this kind of theft, experts in computer science doubt if this stopgap measure will be enough to prevent social media users from more exposure to identity theft (Giles, 2010).

(iv) Accessing the Internet: Laptop Theft

Laptop theft has also lead to more identity theft. Information Week (2009) reported on an incident where the theft of a single laptop belonging to the employee of an insurance trade group put hundreds of thousands of doctors at risk of identity theft. The laptop was simply stolen from a car of the employee. The American Medical Association (AMA) issued a notice to all doctors to be on the lookout for identity theft, in essence a breach of security notification. Nonetheless, this case demonstrated all too clearly how simple laptop theft is, and is yet another front in the war against identity theft, and may well involve police more as it represents a convergence of street crime and high-tech crime at once. Finally, Tomescu & Trofin (2010)

situated identity theft in a still broader concept of “networked publics” where notions of public and private are being reorganized and eroded by the mediated, technological world in which the globalized world operates.

(v) Security Gaps

While a good deal of identity theft currently occurs because of gaps in the security of credit card use in sites ranging from ATMs to everyday stores, resulting in researchers like Smith (2009) calling for new preventive approaches to close these gaps, it appears from the research that the most challenging nature of identity theft is emerging on the internet. Given that credit card fraud occurs in real-time and real-space, application of situational crime prevention methods would not be much different than dealing with other types of place-based theft; applying this model to the internet is another problem altogether.

(c) Who are the IdentityThieves and How did They Acquire the Skills that are Needed to Commit Identity Theft?

Copes & Vieraitis (2007) studied the question of identifying who exactly are identity thieves, and how they came to commit the kind of crime they do. They interviewed 59 identity thieves incarcerated in federal prison to gain some insight into this understudied issue. They found that identity thieves derive from a diverse group, from both working- and middle-class backgrounds, some lead street lives, others respectable middle-class lives. The motivation was primarily based on a need for quick cash, and the perception that identity theft fraud was easy, with few consequences. In terms of how they committed their crimes, most of the information was acquired from others, stolen from mailboxes or trash cans, or obtained from contacts. Buying information entailed buying it from corrupt employees of various businesses, while

dumpster diving is a well-known basic strategy leading to ID theft. A surprisingly common method of obtaining information was from family or friends, who extracted information from parties with the full knowledge of the party. One third of offenders used their employment to commit their crimes, as, working for mortgage agencies, government agencies, such as the DMV, or businesses with access to credit card or social security numbers, they had access to information. Two-thirds of offenders had a prior arrest, about half for previous identity theft crimes, a quarter for drug sales and a quarter for street-level property crimes, a finding which indicates that identity theft is viewed as yet another form of property theft and may result from a continuum of crime due to escalation or search for bigger pay-offs.

(i) Mechanisms Used by Fraudsters to Commit Their Crimes

Fell (2006); reviewing the research, found that, by and large, identity theft is a white-collar crime in which offenders conceal their own identity in order to obtain information leading to the theft of another's identity. Three primary methods for gaining data for use in committing identity theft have been identified: dumpster diving, or stealing information from trash, either in personal or business sites, shoulder surfing, which entails looking over a person's shoulder while they enter in a credit card number, on an ATM machine or by phone, or eavesdropping on conversation, and pretext calling, in which a call is made and the offender pretends to be the bank asking the victim for information, or even pretends to be a victim calling a bank and asking for information. The inside job is another method often used, entailing collecting information from a fellow employee. With regard to online identity theft, hacking of personal information, phishing and skimming, in which "employees such as waitresses and cashiers use scanners sold on the Internet to steal personal information" (Fell, 2006, p. 1). With regard to types of identity

theft crime, the complete borrowing of another person's identity to gain access to credit cards and a lifestyle requires a high commitment level and planning, and is rare. On the other hand, low level of commitment and an opportunity to commit a crime, such as giving an officer a false ID when stopped on the road, is more common. Most identity theft crime, however, is undertaken for financial gain, that is, withdrawing money from accounts illegally. Gaining a job using a false identity is again a task that requires much more planning and commitment. Identity theft is also fed by opportunities provided for it by information users. With regard to students generally, research has reported that while on campus they easily provide social security numbers, they do not create non-obvious passwords, and they generally lack the necessary level of education to undertake corrective action to conceal their identities when using credit cards (Fell, 2006, p. 1).

The methods utilized by identity fraudsters are many. To obtain Social Security Numbers, fraudsters often go dumpster diving in trash cans of businesses, looking for documents on which the SSNs are inscribed. Mail theft is another way in which sensitive personal information can come into their hands. Phony change of address forms sent to the post office can redirect personal mail to illegal sites. Pretexting is an illegal method to obtain information by phone with the offender posing as a telemarketer (phishing is the online version of this, using email solicitations to false web sites, or eliciting payments to bogus PayPal sites). In terms of methods, a number of offline non-technology methods are viewed as a means to an end, which is online crime. In terms of offline methods, 28% of information is gained from stolen wallets or checkbooks, 11% from friends or relatives with access to information, 8.7% from offline transactions, 8.7% from a corrupt employee, 8.0% from stolen mail and 2.6% taken from

garbage (Berg, 2006). In terms of online methods, 5.2% of ID theft occurs through computer spyware, 2.5% from an online transaction, 2.2% from hacking or a virus, and 1.7% from phishing. Berg (2006) reported, five years ago, that online schemes generally reap less profit than offline methods, with, for example, phishing yielding $2,320 per theft versus $9,243 per theft taken from stolen mail. Additional and recent scholarly information regarding phishing and stolen mail profitability remains dated. However, scholars and researchers continue to focus on techniques to detect and counter phishing emails (Dazeley, et al.; Devaluation, 2010).

Most of the offenders used the stolen information to produce additional documents such as driver's licenses, which would lead to bigger crimes, write fake checks, if they were good at forgery or knew a forger, and obtain credit cards or loans (Copes & Vieraitis, 2007). Few of the offenders interviewed expressed any consideration of getting caught, with most of them believing that, given the current state of prevention, the odds of being caught were minimal. Most justified their crimes by arguing that they were victimless, that they were helping others, or that as they worked in groups they were not individually culpable for the crime. The set of skills developed by them to be able to commit these crimes included social skills, technical skills, intuitive skills and knowledge of the system. Social skills included the ability to manipulate social situations, intuitive skills involved being more aware of surroundings and likelihood of being caught, technical skills included the ability to produce or have produced fraudulent documents ranging from checks or credit card applications, while system knowledge entailed a full knowledge of how banks or credit agencies operated and knowing the habits of most stores in surrounding areas with regard to their identification requirements when cashing checks. Most

offenders felt that armed with their skills, they could commit identity theft crimes with impunity (Copes & Vieraitis, 2007).

(d) The Impact of the Criminal Justice System on the Rate of Identity Theft

The strategies of the executive and the legislative branches of government to address the challenges faced in the effort to detect, investigate and combat identity theft and to highlight how much attitudes about identity theft have changed in a short time, is worth looking back briefly at pre-2005 attitudes. Computerworld (2005) reviewed identity theft incidents and responses in the pre-2005 era, finding evidence of some reluctance by companies to address the problem effectively. For example, while Bank of America reported theft of credit card data of 1.2 million customers, industry response was mixed. Some experts felt that such theft required that all data be encrypted to back tapes, while others held firm that existing data-protection rules were still effective in preventing most breaches. Nonetheless, it was about this time that incidents of data theft and identity theft created enough attention that many financial services firms began to "roll out greater data-protection schemes" (Computerworld, p. 10). These included more encryption, content-monitoring and content-filtering methods. The creation of encrypted data on backup tapes generally was resisted, however, because this albeit safer means of securing data required too much processing overhead and was therefore deemed too costly. One expert felt that companies could reduce data breaches by tightening up password permissions and end-user privileges "to prevent theft by disgruntled workers or former employees" (Computerworld, p. 10). The general attitude, however, was that major reports of theft were one-off issues, and not yet patterned or systemic. While this appeared to be the general attitude at that time (a stand which could not be justified in light of increased amounts of identity theft in the five years since),

Computerworld (2005) also reported of a number of major corporations who had taken on the task of encrypting all data on backup tapes in a way that would guarantee that data would not be lost from theft, or company data hacked. Nonetheless, it was also reported by Bank of America that some of these backup tapes had also been stolen. In short, a report from just seven years ago almost seems like it comes from another world, as many of the doubts over whether or not identity theft was here to stay have, in the short time since, vanished.

(i) Legislative Response

The primary response thus far by law enforcement to identity theft, particularly on the internet, has been by passage of laws, either formulating a definition of the nature of the identity theft crime, or providing for actions which must be taken if breaches of security are detected (Burdon, 2011; Coats, 2008; Glithero, 2009; Winn, 2010). For example, Burdon (2011) examined the effectiveness of data breach notification laws, which are described as having been successful in reducing some crimes. At the same time, data breach notification rates have only highlighted the fact that most of the information security practices in corporate culture are as yet inadequate. Burdon (2011) argued that data beach notification laws were created without consideration of a more comprehensive data protection framework. As such, data breach notification laws take corporate compliance cost burdens into consideration too often, by contrast to comprehensive information privacy laws, which adopt rights-based protections favouring individual rights over corporate requirements. In both frameworks, however, the disregard of the crucial role of social contexts and relationships often undermines the efficacy of the laws derived from them.

Burdon (2011) argued that in order for laws to protect consumers from identity theft a greater emphasis needs to be placed on social relationships as opposed to the specific types of information being regulated. Reviewing the development of current notions of protection, Burdon (2011) found them to be based in a concept of information privacy linked to control theories of privacy, defining privacy as an individual's choice to disclose personal information. In the control theory of privacy, privacy is parsed as consisting either of solitude, intimacy, anonymity or reserve, with the latter especially implying a psychological barrier against unwanted intrusion. The mental space of the personal, incompletely communicated to others, necessitates, moreover, the ability of a person to retain private information. In terms of society, privacy supports personal autonomy, emotional release; self-evaluation limited and protected communication, with the latter again setting boundaries to information exchange. Thus, a classic definition of privacy entails both reserve and limited and protected communication, as such, "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Burdon, p. 69). This definition resulted in information privacy law focusing on the right of individual to control their personal information both in terms of what they divulge and who can have access to it. This definition, while critiqued by some, has become the basis of all information privacy legislation passed since the 1970s.

Data breach notification laws only emerged in California about a decade ago; requiring institutions to alert individuals that an unauthorized attempt was made to access their personal information in the company's system. The purpose of the law was to allow individuals to act against identity theft in a timely manner and linked data breach notification and identity theft mitigation due to a major identity theft incident in California's public sector at the time. The

laws hoped to make consumers more aware of the threat to their information-based identities, and secondarily to encourage companies to adopt more useful encryption technologies in the storage of personal data. However, Burdon (2011) found many tensions in these laws, not the least of which is corporate reluctance to advertise security breaches or risk customer loyalty by informing consumers of breaches. In terms of laws passed influenced by California's act, most sectoral information privacy laws have been criticized as sporadic and reactive, while comprehensive laws appear to have trouble being implemented. All laws also come with assignment of duties to various supervisory authorities assigned to protect the rights of individuals and impose compliance on organizations. The U.S. generally does not have a dedicated supervisory authority for information privacy enforcement, with public sector response to identity theft described by Burdon (2011) as fragmented.

Too many corporations, moreover, have devised encryption exemptions which reduce corporate compliance costs incumbent upon the laws. The political balancing act between protecting identities and reducing corporate compliance costs has resulted in compromising revisions to laws in many states, reducing the effectiveness of this approach. Using examples of the Pfizer and ChoicePoint data breaches, Burdon (2011) argued that at present the process-based chains of accountability inscribed in the laws are limited due to the simplistic conceptualization which fails to account for the complexities of personal information exchange and user only remedial rubrics which address vastly different breach situations in the same manner, making them ineffective. Most data breaches, however, emerge in different ways and contexts, demanding differentiated responses. One involved a disgruntled employee, another a mistaken authorization due to the failure of a security system, only in one other case was a third party identity theft criminal actively involved. Thus, the one-size-fits-all approach to data breach

notification only imposes one-dimensional remediation that provides limited help or redress, through narrow chains of accountability. Moreover, in such extreme forms of data breaching beginning to occur, such as Wikileaks, the binary chains of accountability which form the basis of most laws, seeing breaches as between personal information providers, collectors and re-users, breaks down, and as a result there is no form of redress. As a result, Burdon (2011) argued that simple notification of breach is not enough: a strategy must be developed with "would require deeper contextual analysis that is conducted on a case-by-case basis" (p. 106). Moreover, there is "the need for context dependent approaches in classifying personal information that go beyond the information itself and require an examination of the social context of information generation" (Burdon, p. 110). Burdon (2011) found that while laws in New York State and others constrain the notion of privacy, the Australian Privacy Act may in fact be a right step in this direction. With the current focus on the regulation of information to mitigate social harm, this form of regulatory perspective would remain difficult to introduce. Two points relevant to the current study can be extracted from these findings. First, that the law in a particular state will create a framework for law enforcement response to identity theft, and if it constrains the definition of privacy it will result in constraints on police response. At the same time, Burdon's (2011) call for a more contextualized response to data breaches would appear to call for an approach to the crime of identity theft based in criminal theory such as routine activity theory (see below), where the space and time of the crime is a major element in devising ways to prevent recurrence. Thus, the context-oriented nature of situational and routine activity crime prevention methods may provide what Burdon (2011) calls for in terms of improving the legal and law enforcement-based response to identity theft, or at least data breach.

Whether or not identity theft can be legislated away, however, remains an issue of some debate. Coats (2008) reviewed a case of identity theft where reform of state law on the degree to which personal information could be divulged in the course of doing commerce was the response. The rationale behind most laws is that government must do more to protect the public from identity theft. Most laws propose restrictions on access to personal phone records or driver's license data, among other similar actions. However, Coats (2008) argued that most laws will not address the more insidious and effective ways that offenders use to obtain personal data, such as dumpster diving outside people's homes or offices. Moreover, most such information security laws are aimed at shutting down Freedom of Information Act-based access to data, and no identity theft criminals make use of that channel to gain identity information. As a result, the closing of public records, which is occurring in all 50 states, is an ineffective response, and also has the negative side effect of making it more difficult for the public to gain access to information. Coats also (2008) argued that media is partly to blame for creating paranoia about identity theft, leading to state governments adopting these easy but ineffective responses.

Garrie et al. (2010) also remained critical of current laws regarding identity theft on the internet, calling the law "noiseless" insofar as it failed to offer victims of identity theft any recourse, or regulating in any way the mining of information (p. 3). Privacy laws, moreover, only protect citizens from invasions of privacy from the government, not from corporations or phishers. As a result, Garrie et al. (2010) argued that "federal law empowers companies, big and small, to mine consumer data with impunity" (p. 3). Spyware is embedded software, for example, that traces a user's activities on the web, including cookies, but expanding now to software that follows one's every move on the Internet. Spyware, unfortunately, includes both beneficial and malicious uses, meaning that its existence, making the internet commerce engine

possible, also inherently puts users at risk. A major problem with spyware is that it operates in relative secrecy, gathering information on user behaviour without the user's knowledge. As such, "spyware blurs the existing line between a malicious virus and an aggressive Internet marketing tool" (Garrie et al., p. 4). Embedding of malicious spyware in computers is relatively easy and getting rid of it, seeing that most computers have up to 100 spyware components, daunting. Garrie et al. (2010) also reviewed current laws which would allow a victim of identity theft to prosecute the perpetrator. In most cases, most of the current laws do not provide users with adequate protections, often because they were written with larger security beaches in mind and thus individual cases fall below the required scale to be eligible for complaint. Though spyware victims therefore have several legal vehicles, "no single action provides the silver bullet" (Garrie et al., p. 10). Lacking a straightforward course of action, most victims of spyware remain vulnerable, and have little legal recourse if identity theft as a result of spyware activity occurs. Garrie et al. (2010) recommended that a statute be developed which requires spyware users to gain consent to collect personal information from Internet users in order to develop their data. This multi-click consent agreement would reduce the unknowing use of personal data for either positive or negative reasons on the Internet, and, Garrie et al. (2010) believed, reduce the opportunity for identity theft. Such an agreement could be written into an amendment of the Stored Communications Actions increasing the requirements for authorization and consent. In addition to amending U.S. law, however, international law must also deal with the problem of spyware as it provides opportunities for identity theft worldwide. Thus, Garrie et al. (2010) offered a legal solution to the reduction of an opportunity for identity theft in a currently routine activity engaged in by most retailers on the Internet.

The Identity Theft Penalty Enhancement Act established in law a new statutory crime, aggravated identity theft, which enforces a two-year sentence for any identity theft. Nonetheless, thus fact that the law has only been made use of, problematically, in the view of Glithero (2009), in immigration law, is only one example of the weakness of the law. This is primarily because the law has been interpreted in too many different ways. An important change in the law occurred in Flores-Figueroa, where it became a requirement of proof of a crime that the person knows that the identity being used belongs to another person. While this stipulation more or less ended use of the law in immigration contexts, it presented still more problems. In reviewing the implementation of the law before and after Flores-Figueroa, however, Glithero (2009) still found that the law leaves many victims of identity theft without legal recourse.

There remains considerable debate about the ultimate effectiveness of breach notification laws (Winn, 2010). Some argue that these laws are too permissive, others than they are too punitive in nature. Winn (2010) argued that a major problem is that breach notification laws "provide no framework within which public-private collaboration can take place to improve compliance over time" (p. 1158). That is, breach notification laws leave companies to "navigate the maze of competing information security product vendor claims with few reliable standards for guidance" (Winn, p. 1158). Nor do the breach laws allow for any general rating of overall company response to data theft, naming them either as exemplary or lax. That is, the one-size-fits-all approach of the law blunts its accuracy. For this reason, Winn (2010) proposed a number of regulatory adjustments to the current breach notification laws, hoping to fine-tune them for effectiveness.

(e) Corporate Response

(i) Red Flag Rules

The high incidence of identity theft, and the fact that it is a growing problem, caused Congress to pass the Identity Theft Red Flags Rule in 2008, which requires all companies to implement a written identity theft prevention program to identify and detect warning signs of theft, so-called red flags (Bose & Leung, 2009; Clapper, 2010). The law applies to all companies who make use of consumer credit information. Companies must not only identify red flags, such as suspicious patterns of activity, and data discrepancies suggesting an ID may be fake, but must put in place processes to detect and alert the company to red flags. They must also have a list of actions that they intend to take to respond to red flags, and undertake as well a periodic evaluation of the effectiveness of their red flag program. Curtis (2011) found some confusion in the red flag rules, and was not clear as to the capacity of most companies to develop red flag policy. Also, "whether (companies that use red flag policy) are subject to an actual reduced risk of facilitating identity theft remains to be seen" (Curtis, p. 14). Nonetheless, the fact that companies need to develop preventive policies opens up a channel where they can consult with law enforcement to help them develop a red flag policy. By and large, the red flag rule paradigm in response to identity theft places the responsibility of reduction of fraud on companies themselves, with the companies developing better security. Whether or not this remains a realistic possibility, especially in light of the internet location of most identity theft remains a problem. Nonetheless, many studies address identity theft from the perspective of what companies or sectors can do to reduce the problem on their own.

Indeed, the possible problem inherent in red flag rules, that they place a significant demand on companies, was only further reinforced by the fact that the implementation of the red flags rule had to be delayed to give companies more time to develop and implement written

identity-theft prevention programs. The Federal Trade Commission also had to create and release a template for an ideal compliance program to expedite the process of company policy creation. Clarification was also needed as to the definition of a creditor or persons whose data companies must take care to protect. A creditor was defined as a party who regularly extends or renews credit for goods or services. A single credit card use does not make a customer a creditor under this definition, therefore, the companies would be released from responsibility of protecting such data. The Federal Trade Commission also had to create a website to help companies work through the requirements of the law and embed them in identity theft prevention programs, all efforts undertaken by government which cast further doubt on the ability of companies to handle identity theft on their own (DVM, 2009).

Red Flag rules were introduced by the Federal Trade Commission in November, 2007, mandating that companies instituted prevention and detection programs to control identity theft. But delays in implementation have occurred, not only because commerce in general balks at creating such plans, but because specific industries, like the healthcare industry, have lobbied against their responsibility in the matter. Identifying the various red flags that might occur in each industry has also been a more conceptual challenge. For example, Lee (2009) described a few of the potential red flags that might emerge in healthcare contexts. These would include an apparently altered ID, a problematic photograph, inconsistent data on cards or forms, suspicious changes of addresses, apparently fictitious addresses or phone numbers, a complaint by a customer about another patient's bill, claims that bills were not received, or any alerts to consumer reporting agencies. Inconsistent medical records would be another example of a red flag. As a result, red flags as a rubric generally entail personnel receiving data from consumers detecting any irregularities in the data provided them, or responding to suspicious inquiries from

consumers related to patients. A red flag program would then provide protocols for how personnel would proceed if such red flags were detected, and what they should do to stop the potential for identity theft based on suspicions. Red flags, therefore, in fact emerge out of routine activities in terms of provision of data in consumer interaction, but may be limited to the extent that it is based on suspicions about the nature of data presented (Lee, 2009).

Only financial institutions and creditors that offer what are termed covered accounts (or accounts involving repeated ongoing payments by means of credit) are subject to Red Flag rules. After its original conceptualization, the Red Flag Program Clarification Act (2010) had to be signed into law to clarify for all which firms are subject to red flag rules, and which are not, in effect exempting firms like medical offices and law firms that only incidentally accept credit in payment for services. Indeed, McMillion (2009) reviewed in some detail the argument made during lobbying by the American Bar Association that lawyers should be exempt from red flag rules primarily because they do not qualify as creditors under the definition of that term in the law (meaning that while they now and then accept credit-based payments they do not in fact extend lines of credit to clients). The ABA also argued that insofar as most law firms are relatively small, the red flag rules would impose burdens on them that would not translate into any measurable benefits for clients. These lobbying efforts were successful, as in the above clarification of the red flag rules lawyers were exempted from the law. Kunick & Posner (2011) also argued that, by and large, few companies have the in-house skill set to develop red flag rule rubrics, meaning that information management professionals will have to be hired.

Red flags fall into three categories: alerts or warnings from a consumer reporting agency, the presentation of suspicious documents, the presentation of suspicious personally identifying information and unusual use or suspicious activity on an open account. A red flag program must

monitor the account for these red flags, contact the account holder if there is a red flag, request change of password to block suspicious use, close current accounts and open new accounts for patrons, refuse to collect on red-flagged accounts, notify the appropriate law enforcement authorities, make a notation on the account that the red flag incident has been taken care of and update the prevention program to reflect the ever-changing risks in the identity theft field. Information management professionals are required to create and manage such a system insofar as they will intersect with complex technical issues, meaning that the information management professional serves as a go-between between the program and the technological issues involved. Kunick & Posner (2011) presented a scenario where an optimal red flag program managed by an information management professional will be effective in reducing identity theft. His description of the program also detailed how in-company management of identity theft intersects with law enforcement, insofar as law enforcement is one of the required entities to whom red flags should be reported. Thus, the red flag rule laws may well have established formally the basis for a cooperative response to identity theft between in-house information management personnel and law enforcement.

Listerman & Romesberg (2009), however, argued that laws can only go so far to stem the tide of identity theft and that a more comprehensive approach would entail creating a culture of security in a company. He described a company meeting where employees felt free to leave personal belongings unattended, remarking "in a culture of honesty and a high degree of trust, where people are bonded together under a common cause, even open temptation is mitigated by a culture of security" (Listerman & Romesberg, p. 28). Such a culture can be created by identity theft awareness and protection seminars buy in and support of the program by CEOs and offering all employees in one's company an identity theft protection service that will handle all of the

complicated elements following an identity theft incident. By having an experienced professional to attend to all corrective measures that are required to be taken after an identity theft incident, a company demonstrates its commitment to preventing identity theft, and provides the same service to all employees in ways that prevent management from blaming employees for security lapses. Listerman & Romesberg (2009) also recommended that companies create a data security project team, often involving employees themselves. Giving employees ownership of the program will subsequently reduce their resistance to buying-in to the program.

FTC guidelines should also be followed, including taking stock of all of the personal data that the company takes in, and then deciding to stop in-taking or discontinue collecting sensitive information which one deems is not absolutely necessary for the operation of the business. Such scaling down techniques include putting a disposal date on all data, requiring that all sensitive data be deleted after a certain amount of time, to prevent it being exposed to identity theft. Another FTC mandate is to lock up data in physically secure places, ensuring that there is only limited access to it. Disposal should also be done according to strict guidelines set down by the FTC, including taking such precautions as using effective shredders, wiping tossed out computers clean, making sure that remote users of company computers use the same policies or hiring a shredding service management company. Listerman & Romesberg (2009) also included red flag rules in the company plan, and would require all employees be trained in detecting red flags. Overall, however, they extracted from FTC regulations a broader notion that in addition to simple training in red flag rules companies must create a culture of security to reduce incidents of identity theft through company held data.

Another problem with either breach notification or red flag rules is that they do not apply to the federal government itself. If you receive a notice from the Internal Revenue Service (IRS)

reporting that a refund was delayed because identity theft use of your social security number was detected, the IRS is not required by law to do more than notify you, and leaves the taxpayer with no way to prevent further tax-related identity theft (McKee & McKee, 2011). This remains true even when there are up to 1 million tax-related identity theft reports per year, 40,000 of which are investigated by the IRS each year. Indeed, identity theft has been used to file fraudulent tax returns, can create penalties for taxpayers and invalidate one's social security number—and then there is the delay of a refund. While the specific purpose of McKee & McKee's (2011) review of tax-related identity theft and fraud is to provide tax preparers with a list of very specific and highly technical red flags which only occur in tax payment contexts, their review of the problem of identity theft in the context of tax payments clearly indicated that experts in the field are required to detect red flags in specific types of forms. That is, tax preparers themselves must be proactive in alerting taxpayers to identity theft as "taxpayers are frequently overwhelmed with the detailed and time-consuming steps required to correct their records and prevent future problems" (McKee & McKee, p. 55).

One of the most common sources of identity theft is related to credit or bank cards. For that reason, Clapper (2010) described in detail how data is stored on bank cards, and how data was stolen from card use by customers of the Hannaford grocery chain in Massachusetts in 2008. Identity theft is distinguished from credit card fraud in that while the former demands that personal identifying information be stolen, credit card fraud only requires a stolen primary account number. In both cases, in card-present situations this crime is risky, though "it is much less risky for the fraud perpetrator if they can do their fraud over the Internet, rather than in a face-to-face setting" (Clapper, p. 122). A fraudulent credit card can be used with some ease in making illegal purchases from an online site, for example. For this reason, Clapper (2010)

recommended that all websites should require buyers to enter the CCV2 value and the PAN and expiration data, to increase security. One interesting aspect of the Hannaford case was that they had much better security than most comparable businesses, and thus were not found to be at fault for the loss of customer data to fraud.

Finally, the last dimension of identity theft involves what the criminal is able to do with the fraudulent identity after the theft: this too can be limited by enforcing simple security measures or by redesigning cards to make them less accommodating to fraudsters. Overall, then, Clapper (2010) also adopted a remedial vision of how to stop identity theft in current routine behaviour: that is, improve the security elements of most cards, and limit the degree to which cards can be used, and identity theft will be less damaging to customers who are victims of fraud.

Dunn (2011) also addressed the mandate that breaches of security be reported as a method of reducing further incidents of identity theft. A breach of personal information must be reported, in the context of the U.S. Army, to the U.S. Computer Emergency Response Team within one hour, as well as reported to command. Affected individuals must also be notified. Dunn (2011) found, however, that too many breaches continued to occur. In exploring the issue, he found that "military agencies routinely use social security numbers for a number of purposes, often without good reason" (Dunn, p. 37). This then leads servicemen to be vulnerable to identity theft. Efforts to reduce the use of SSNs in military life have proceeded, first through a review of all official forms used by the DOD to ensure that SSNs are required only when necessary, and then by the creation and adoption of alternative forms which do not require SSNs in the "most routine business practices with DOD" (a phrasing which specifically echoes routine activity anti-crime theory) (Dunn, p. 37). The goal of the initiative was also to eliminate the use of visible SSNs from DOD identification cards, replacing SSNs with DOD identification

numbers which are less susceptible to identity theft. Insofar as this preventive measure involved a reform of a routine activity from which it was determined that circumstances favouring identity theft emerged such a change could be said to comply with the guidelines of criminal routine activity theory prevention.

(ii) Victim Awareness

While breach of notification does not seem to be ideal in stopping identity theft, then, it is possible that combining this approach with other elements may add up to a comprehensive preventive approach. For example, Domonell (2011) addressed the problem of identity theft in a population of college students. The EDUCAUSE Higher Education Information Security Council has issued guidelines to help colleges build up protective measures to prevent identity theft on campus. Universities remain, however, targets for identity theft hackers. For example, the University of North Carolina, Chapel Hill, has 60,000 IP addresses connected to it, and wards off 30,000 hacking attempts per day, every day. To help in this process, the council recommended that universities hire consultants in vulnerability management, compliance and penetration testing solutions for the internet to reduce crime. Consultants inform colleges how to address security issues by taking the hacker's perspective on current practice, to identify weak spots. Some colleges have adopted the use of the Identity Finder software, which scans through all student data, identifying where sensitive data is contained in records, and deletes it when required to ensure that student information is not exposed to hacking. Devices that protect credit card use on campus have also been installed, with some Universities creating their own separate networks to prevent theft. Many have sought to update their compliance to the Payment Card Industry Data Security Standard, and often turn to consultants to identify gaps in current compliance. Awareness training, for all personnel and students, so that all citizens are aware of

the extent of the identity theft problem, is yet another approach being used to reduce incidence of identity theft on campus. All faculty, staff and students at the University of Houston, for example, are required to take a course on social media security. Social networking in particular has been cited as a place on the internet that remains risky, because of the trust built up in communities of "friends" who share information with each other. The implied trust in Facebook and Twitter often results in more youth going to spoof hacking sites than other populations of users. Here, too, notification of security breaches is still another way in which universities hope to combat the problem, again working on the premise that awareness will reduce careless behaviour leading to theft. In sum, the battery of responses include: always asking why social security numbers are being requested, understanding where information is stored, storing information under lock and key, training students to understand the power of personal data and improving awareness. As will be seen, many of these strategies appear to derive from situational crime prevention strategies to prevent other types of crimes. Domonell (2011), however, did not report on whether or not implementation of these measures improved data security and reduced identity theft at the targeted universities.

Whereas victim awareness programs are one of the major ways in which enforcement seeks to limit the opportunity for crime, according to the situational crime prevention model below, it could be argued that any efforts to create a security governance framework designed to strengthen company compliance to standards or protocols for Internet or data security, on behalf of the reduction of identity theft, would be another variation of the same strategy. That is, compliance reduces the opportunity for crime. Nicho & Fakhry (2011), however, found that in spite of the fact that companies and industries as a whole have created standards, such as the Payment Card Industry Data Security Standards, and have imposed penalties for non-compliance,

it remains difficult for many companies that make use of credit cards in their daily business, especially small companies, to comply with the standards. The most commonly cited reasons cited for failure to comply include the high cost of implementing the standards, and the increasing difficulties faced in both the interpretation of the standards and the application of the standards to individual businesses. One of the most vulnerable areas for identity theft, because companies most often fail to comply with standards, is the storage of cardholder data. Nicho & Fakhry (2011) argued that by and large one of the major difficulties in compliance is that the standards are governed in an industry-specific way, and require a more comprehensive information security framework focused on governance to be more readily complied with. Nicho & Fakhry (2011), therefore, sought to create a more comprehensive framework by combining the existing credit card industry standard with Control Objectives for Information and related technology (COBIT) standards and the Technology Infrastructure Library (ITIL) and ISO standards. The purpose of the combination would be to increase the functionality of the standards and provide them with extra layers of protection, offering companies a defense-in-depth approach to security. In essence, this framework would increase company awareness of the importance of complying with security principles, offering, then, an SCP framework response to the problem of companies providing identity thieves with an opportunity for crime in unprotected cardholder data (Nicho & Fakhry, 2011).

Otto (2009) quite succinctly summarized the ongoing debate, then, in how to best control identity theft as a conflict over whether or not *rules* or *standards* are the best approach to prevent identity theft (rules being protocols created by law or companies, standards created by industries or fields). In the area of software, Otto (2009), reviewing rules versus standards issue, argued that the nature of software development makes it almost impossible for software engineers to

come up with lasting security and privacy rules, meaning that while they might be more comfortable with rules, it is only broader regulatory standards frameworks that, complementing technical expertise, will improve online security and benefit society. The software engineering community has also struggled with obtaining compliance from users of their products. There is also a divide between legal requirements of compliance and engineering realities, which raise other concerns about the effectiveness of data security and privacy protections.

While lawmakers pass legal mandates for compliance, the technical means to establish and maintain compliance continue to lag behind. Thus, cases have emerged where citizens ostensibly have the protection of law to safeguard their private data, but the software systems managing the data are "ill-equipped to provide the protection without the possibility of unauthorized access" (Otto, p. 315). In this gap, much identity theft opportunity occurs. Paradigmatically, then, Otto (2009) clearly concluded that all of the above efforts espoused by the information industry to combat identity theft techniques with technical-based countermeasures and rules will not succeed, and that broader behavioural standards must be put in place to reinforce these measures in order to provide true protection. That is, only broad standards, not specific rules, however ambiguous such standards may seem to engineers, are required to maintain security, insofar as broad standards "allow the law to capture moving targets" both by mandating continuing development of security rules and by offering potential victims broad privacy protections (Otto, p. 316). Otto (2009) came to this conclusion after examining the specific opportunities for data theft deriving from specific aspects of the design, development and deployment stages of software production. By understanding these specific characteristics, appropriate safeguarding methods were derived (a method thus echoing the SCP approach). The complexity of software, the delays and flux in its development, the flexibility of

software, the ability to add new functionality, the ease of replication, the automation of software, the full use availability of designed software, its ability to handle large amounts of data, lack of transparency in its accessibility decisions, and the existence of problems in software even after deployment, all make software profoundly different to physical objects, and create opportunities for theft. They also make it much more difficult to regulate software and compliance to security rules, though specific rules allowing or prohibiting specific software elements have attempted this approach of security protection.

(iii) Standards

Rules for encryption, allowable transactions, software development proscription and others, as a result, cannot be effective, since they cannot plug the gaps in the nature of software development and operation. Thus, Otto (2009) analysed the opportunity for crime in the specifics of software contexts, and decided that standards were the best preventive approach to reduce software-based data and identify theft. To the extent that standards demand compliance and compliance is often enforced through preventive awareness-based training, the preference for a standards-based approach to online security offered opportunities for application of the situational crime prevention framework to the security paradigm.

(iv) Rule Proliferation

In addition to research supporting the application of various rules or standards, including red flag rules, the development of FTC standards, the Health Information Portability and Accountability Act (HIPAA), as well as its Privacy Rule and the PCI DSS, all raise the potential for confusion in compliance, due to the proliferation of rules (Rubens, 2009). The HIPAA rules,

in particular, are typical of the confidentiality rules imposed upon fields, in this case the healthcare field, to manage personal data and prevent identity theft. While acknowledging that such standards protect data privacy, Wartenberg (2010) also pointed out that these sorts of confidentiality rules have had unintended negative consequences on the conduct of public health research and practice by making it more difficult for researchers to access necessary data for research. Thus, once again, privacy and public interest exist in a tense relationship with each other. Wartenberg (2010) focused in particular on restrictions to access to routinely collect personal medical data, the restriction of which restricts epidemiological study. The kind of professional resistance to further restrictions on limiting access to personal data thus represents a significant barrier to providing fuller protection against data (Wartenberg, 2010).

(v) The technological Solution

In addition to the above approaches, industry in particular seems intent on hiring technological experts to device defensive technology that will combat Internet-based identity theft. Phishing, for example, remains one of the most common means by which identity theft is undertaken online. Miyamoto, Hazeyama & Kadobayashi (2010) tested a new approach to reduce identity theft on the Internet by finding a way to identify phishing sites. HumanBoost, a program that improves the accuracy of detecting such sites based on users' past trust decisions, was examined in a case study of 10 participants who browsed 14 simulated phishing sites and six legitimate sites, and made decisions about whether or not the site was phishing or not. The trust decisions made in this context by the users, entailing decisions by consumers about whether or not they wanted to share personal data with the site, were then converted into a heuristic and tested through HumanBoost. The average error rate of the ability of HumanBoost to detect the

presence of phishing sites was below other programs, meaning that HumanBoost has the potential to improve detection accuracy for browsers. Thus, the study found a way to program a heuristic that could help users stay away from phishing sites, hopefully disabling their malicious intent in terms of identity fraud. Again, Miyamoto et al. (2010) strongly imply in their results that only by improving the Internet in terms of security technology will consumer vulnerability to phishing and identity theft be reduced.

(vi) Biometrics

Al Harby et al. (2010) described an example of the use of biometric devices to increase security in an e-commerce environment, with particular interest in user acceptability. They specifically focused on the use of biometric devices to improve security in banking log in access, where identity theft, hacking and virus problems have increased dramatically. According to studies, 8.4 million Americans reported having their identity stolen in 2007, and the loss based on complaints of identity theft amounts to $239.9 million to banks (Javelin Strategy & Research Survey, 2007). Biometrics is advanced as a solution to the inadequacy of current security methods in that a biometric device uses a unique biological trait to distinguish the user and, as such, rises above some of the vulnerabilities of the current security system. Biometric-based security, to the extent that it is based on something you are, as opposed to a knowledge-based password and object-based token security, is believed to be more effective than current security conventions. Fingerprint recognition is the most popular form of biometric measurement, because they are low cost, reliable and highly accurate. Biometrics has even been introduced to improve security in online banking. Whether or not users will accept the idea of providing a computer system biometric data remains an issue. For that reason, Al Harby et al. (2010) made use of the technology acceptance model in order to examine whether or not a population of bank

users in Saudi Arabia would make use of biometric security. The models measure users' perception of usefulness, attitudes towards usage, perceived ease of use and behavioural intention to use, interacting with new product attributes to determine if users accepted this technology. The results found that perceived ease of use and perceived usefulness had the greatest positive impact on use of the system, meaning that if users perceive that biometrics will provide them with greater security in certain situations they will make use of it. The results of the study, then, established that, if users perceive security as a major issue, biometric security may be a viable way to improve current security methods and greatly reduce identity theft carried out through the Internet or at sites, like banking ATM machines, where technology and user identification come together.

(vii) Accountability

Aggarwal et al. (2010) argued that the main reason for such a high incidence of identity theft on the internet is a lack of accountability in internet systems. They, therefore, proposed a trust management framework, imposed in a complementary way in support of security models that they argued would be able to enhance accountability. The framework includes four trust-based accountability measures: identification, authorization, attestation and retribution. While trust is a basic element of most commerce, Aggarwal et al. (2010) found that on the internet the concept has been elusive, and that most internet systems are far from trustworthy. The fact that emailing more or less accepts the fact that it is plagued by spam, regardless of filters, and the recognition that phishing is also likely to occur, means that the trust level in emailing is low. This then means that users must be extremely careful in terms of updating anti-virus programs and opening any emails from unknown parties. The fact that most identity laws do not apply to

the context of the Internet also places users at risk of identity theft. Current security, focused on confidentiality, integrity and availability, ensures that data is confidential, not altered by the system or suspect to attacks by hackers, and is therefore not enough to ensure protection from identity fraud in an untrustworthy environment. Based on distrust of users, most security at present acts reactively to countering specific threats. Some elements of current security methods, including the anonymity, perfect forward secrecy and plausible deniability aspects of Internet use, can even be exploited by attackers. One of the main problems with the internet is that it was originally conceived as a place where willing users cooperated in healthy ways, without concern for issues of trust. The internet then evolved into a much more complex and dangerous place. As a result, having trusted in other users early on, when that vanished, trust vanished, resulting in the current state of security-conscious Internet. But Aggarwal et al. (2010) argued that by managing trust, through a trust-management model that keeps track of each peer's measure of the trustworthiness of its peers, a degree of accountability can be established. They demonstrated how this would be done by adding a more detailed degree of granularity to the components of identification, authorization, attestation and retribution. These combined to create a Trusted Mail Transfer Protocol which defines a set of attributes whereby the email is evaluated as to its credentials and trustworthiness. Aggarwal et al. (2010) argued that this method is superior to the current paradigm and especially current data security laws, which are mostly based on reasonableness standards and do not "attempt to micromanage technological data security practices" (p. 12). The use of acceptable use policies, filtering and blocking of traffic has not deterred the growth, for example, in spam, which now entails up to 90% of most emails, and increasingly contains viruses and worms.

According to one report, Google email security blocked 100 million viruses every day during the year 2009. Moreover, spamming has become more complicated, as "users who unwittingly open email attachments containing malware aid spammers who add their machines to botnets, a network of hijacked computers that can then be used to send more spam, to launch DDoS attacks, and to commit other crimes" (Aggarwal et al., p. 12). Through a combination of the CAN-SPAM Act of 2004 and state laws against spam some success has been had in fighting spam-based stock fraud and identity theft. But Aggarwal et al. (2010) argued that this model too cannot keep up with the growing amount of spam-based malicious malware, and a new paradigm is needed to address these issues in a more thorough way. By requiring an IP address, possibly third party certification, continuous evaluation of the reliability of the users, curtailing the ability of users to communicate anonymously, identification of all users can be established.

Authorization will then entail a decision-making process to grant an entity permission to perform actions, in essence establishing a contract between users, attestation moreover will be established by collecting and preserving digital documents that can then be used as evidence in a court of law to prove violations of trust, or a criminal act (this would be done whenever a violation of trust occurs). All of these elements of a trust accountability system accord with laws are now calling for all internet systems to preserve data that could then be used in courts of law to prosecute fraud. Retribution can then be exacted in a direct manner without first asking the trustee to have to demand that the violator stop improper actions, mainly through immediate blocking. This is legal because "a private network, such as one at a business, is not a state actor and its actions restricting speech do not violate First Amendment rights" (Aggarwal et al., p. 15). Overall, then, Aggarwal et al. (2010) argued that a trust-based accountability model based on

establishing identification, authorization and attestation of users to enable trust, and exacting immediate retribution if the trust is violated, will do much to counteract the current weaknesses of security enforcement in an untrustworthy Internet environment, especially in light of the exponential increase in spamming and malware attacks in recent years.

(f) Corporate and Law Enforcement Cooperation

The cooperation of information technology experts and law enforcement might be more likely in cases where incidents of computer crime occur on a national level, as, for example, in the case study provided by Bronk (2008) where suspected hacking attacks using botnets to shut down the digital elements of the Estonian government in 2007. Botnets consist of a series of hijacked networked computers that are then used to send direct massive quantities of data to a particular website, causing the system to crash. Exemplary of the problem of formulating a framework for such an incident, it is as yet unclear if such an attack could be construed as a martial act, or an act of cyber warfare (NATO at present does not recognise cyber attacks as acts of war). While continuing to be labelled within the framework of international criminality, Bronk (2008) also argued that these are political actions. Examples of political actions carried out online include Web page defacement in protest of government actions, against nuclear testing too close to certain towns, or even some online actions by the Palestinian Intifada. China appears to be ahead of others in reframing the nature of international online criminality as political action, with a chief military thinker declaring that their military thinking now embraces "a war of knowledge, and a war of intellect" (Bronk, p. 134). Bronk (2008) proposed a new framework which acknowledges the degree to which an international cyber community fashioned by information technologies often bypasses traditional interstate diplomacy and

security channels, forcing states to deal with so-called “intermestic security” (intermestic combining international and domestic) on a whole new level. To provide some perspective on the changes underway at present, Bronk (2008) reviewed the gradual reshaping of statecraft by industry and commerce over the past two centuries, culminating in an industrial age conceptualization of state secrecy based on controlling information flow, creating secret codes, locking away top secret documents in physical places, necessitating spies or turncoats to gain access to secure places, and circulating sensitive data in organizations only on a need to know basis. This paradigm is now breaking down, in the age of electronic communication. This requires a new model of risk, little of which has emerged.

Globalization is defined in this context as “a gradual and ongoing expansion of interactive processes, forms of organization and forms of cooperation outside the traditional spaces defined by sovereignty” (Bronk, p. 139). At present, no transnational policy framework has taken shape to regulate and protect networks from electronic eavesdropping. Moreover, few nation states have developed sophisticated security policies, and only the Council of Europe has sought to define cybercrime, though Bronk (2008) argued that their definition continues to overly focus on traditional conceptions of criminals. By contrast, the global communications systems are “an anarchic system in which all manner of negative externalities have occurred due to unforeseen activity” (Bronk, p. 141). According to neoliberal theory, states should cooperate to form an international regime that bans cybercrime. According to neorealist theory, however, each nation would have to develop its own institution for information defence to stand beside its military to defend a particular nation state. In this scenario, “information warriors would patrol segments of the global information grid falling inside the borders or interests of their respective

states defining against each penetration and possibly responding to them by zapping the sources of attack by electronic means" (Bronk, p. 141). A further example is found in the United States constitution which shows the President as commander and chief of the Army and Navy. Society has expanded and the President is now in charge of the Air Force and Marines. These two examples are proffered as an example of the world expanding in a comparable manner to the technology expansion, providing an avenue for cyber space theft. Bronk (2008), reviewing these models, argued that the reality of international cybercrime may result in a situation that falls somewhere in between, again primarily due to the fact that so much cybercrime takes place in globalized ways. States therefore cannot hope to defend themselves alone from cyber attack without collaborating with private sphere firms to develop expertise. A networked system, entailing collaboration by any number of enlisted organizations, would be necessary to create a new level of security for information. Each part of the network will maintain its security on an individual level, creating in sum security for the network as a whole. States would play a role in the creation of this networked solution primarily through their power to marshal forces and finances in order to mobilize resources both in government and in agencies and organizations outside of government. Thus, Bronk (2008) essentially provided a conceptual framework for globalized defence against cybercrime that necessarily includes government regulation and law enforcement involvement in the prevention of all cybercrime, including identity theft.

(i) Police Response

Police and technology experts in the United States have collaborated thus far to combat identity theft in some cases. By and large, police involvement brings to the table a host of criminological theory and crime prevention practice which is the focus of this report. Many of

these approaches appear to offer more promise for preventing and combating identity theft than defence mechanisms underpinning legislative and company responses. For example, Greenwood (2009) described an incident in North Carolina where police recovered a stolen laptop, which subsequently led them to uncover an identity theft ring. The laptop had Absolute's Computrace Agent embedded in its firmware, which helped to recover the specific laptop and also uncovered the ring. The latter was done through mining of the forensic evidence left on the computer by the persons who stole it and used it for identity theft purposes. The apprehension of the computer resulted from a combination of technology and police work, with the school notifying both the police department and the Absolute Computrace subscription service. The Computrace, embedded deep within the computer, allowed the police to contact the computer and ask it to send updates on its location every fifteen minutes. The theft recovery team of Absolute then used other forensic tools such as keystroke capturing and registry scanning to learn about the computer's use while stolen. After determining where the computer was, the police organized a raid, which in turn uncovered other evidence leading to detection of an identity theft ring. Thus, Greenwood (2009) extolled this case study as an example of technology and law enforcement working together to solve identity theft crime. However, the complexity of identity theft would seem to necessitate the application of a more theoretically-grounded response to this crime on the part of law enforcement. This is the subject of the remainder of this review.

(ii) Improving Law Enforcement Response to Identity Theft: Situational Crime Prevention and Routine Activity Theory

Whether or not law enforcement itself can contribute to the reduction of identity theft by applying the precepts of known theories of crime prevention remains a question, due to a number of police cultural and political issues that prioritize police work and crime prevention (see

chapter five). This would require applying a theory of crime prevention to identity theft, both on and off the internet, and then determining if the approaches derived from the theory contributed significantly to the prevention of identity theft crime (Boetig, 2006; Miethe & Sousa, 2010).

The situational crime prevention paradigm emerged from the opportunity framework that entails both routine activities theory and rational choice theory, and "was designed to address highly specific forms of crime by systematically manipulating or managing the immediate environment in as permanent a way as possible, with the purpose of reducing opportunities for crime as perceived by a wide range of offenders" (Tillyer & Kennedy, 2008, p. 76). More recent studies have found that in addition to providing opportunities for crime, environments can also provide the motivation for crime. Thus, crime prevention must respond by altering the opportunity structures of crime sites, either by increasing the efforts, increasing the risks, reducing the rewards, reducing provocations and removing excuses. Most situational crime prevention approaches have focused on getting victims or targets to alter their behaviour. Tillyer & Kennedy (2008) listed the battery of methods, including increased effort, which involve group-focused enforcement that makes it more difficult for offenders to enlist co-offenders; increased risk, including proactive intelligence gathering, mobilizing community groups and increasing sanctions against community leaders; reduced reward, which entails undermining criminal relationships that enable violence; and reduced provocation and removing excuses. Focused deterrence approaches to reducing crime have also been popular, though often at odds with situational crime prevention strategies. Tillyer & Kennedy (2008), however, found that both theories shift away from the root causes of crime to situations and environments, meaning that focused deterrence and situational crime prevention frameworks may be complementary, with the former aimed at micro level offender motivation, the latter at the environment. Tillyer

& Kennedy (2008) argued that by combining the two, a still more improved model of crime prevention might be created. Again, focused deterrence involves identifying specifically the key actors who generate crime and then communicating to them the sanction risks associated with their behaviour. By communicating risk and sanctions to the offenders, deterrence approaches reduce crime. Tillyer & Kennedy (2008) argued that the group focus of deterrence combined with situational prevention can improve crime prevention.

The law enforcement literature is crowded with examples of the application of situational crime prevention strategies to reduce crime. Cromwell et al. (2008), for example, described a case study where SCP was applied to the increased incidence of crime in libraries. Insofar as identity theft remains at bottom a type of theft, case studies on the utility of situational crime preventive approaches to countering theft would seem to inform the application of the paradigm to identity theft. This is because according to the situational crime prevention paradigm theft is viewed as a highly opportunistic crime, and offenders are viewed as simply alert opportunists, "who are primed to respond by using short-hand cues to quickly evaluate attractive targets" (Miethe & Sousa, 2010, p. 241). Though not cited by name, in Mensch & Wilkie's (2011) study below, it is apparent that the SCP paradigm was enlisted by colleges to increase student awareness of identity theft online as a way to reduce victimization. This would then represent a convergence of the situational crime prevention framework and identity theft prevention methods.

Again, routine activities theory (RAT) argues that for a crime to be committed it is necessary to have a motivated offender, a suitable target and the absence of a capable guardian. With the loss of any of these three elements in a potential crime scene, the outcome of the crime will be different, or maybe not even occur at all. Thus, the best approach for crime prevention based on routine activities theory would be to interfere with any of these three elements. In

terms of offender motivation, RAT argues that criminals are motivated to choose the victim that requires the least amount of effort, that are obvious, and that are most likely to provide the results they seek. Target suitability entails the likelihood that a person will be attacked by an offender, and is marked by the least amount of challenge, which could be communicated to the offender by any number of careless activities, such as walking with eyes to the ground. Suitability is defined by either value, or the target's worth, inertia, or the physical weight or portability of the target, visibility, or if it is plain sight or not, and access. Targets also become more suitable by their daily habits, such as leaving a home unattended all day. Finally, RAT argues that absence of capable guardianship is necessary to create an opportunity for crime. This can include not only officers of the law but anybody in the vicinity who might be perceived by the criminal as a potential disruption to the criminal act. That is, neighbours, friends, bystanders, even shop or property owners. A busy neighbourhood itself might create a symbolic threat to the disruption of the crime as perceived by the offender. Finally, Fell (2006) argued that the fourth, often overlooked element of RAT, is that all three elements must converge at the same place or time, that is, it takes all three to result in an increase or decrease in the crime rate. RAT, finally, is focused on predatory crime, but argued that "most crime that is committed is ordinary and non-serious" (Fell, 2006, p. 26).

RAT posits that offenders go through a process of rational choice before making a decision to commit a crime, assessing the situation. RAT has been found to explain the likelihood of some populations being subjected to certain crimes, like a woman being stalked, or mugged. But other research has found only moderate or partial support for routine activity theory. By and large, however, Fell (2006) found that RAT is generally deemed effective as a method to prevent crime. That said it has not been applied to identity theft.

(g) Validating RAT and its Elements

Routine activities theory has been one of the main theories in support of crime prevention since its inception over fifty years ago. The model explores crime by examining the components of crime at specific locations in space and time without regard to the criminal's motives. The theory, further developed by Cohen and Felson in 1979, went against then current criminal theory, focused on motivation and environment, by arguing that acts of crime were committed as part of the routine activity that develops at a certain site or through daily patterns or activities of social interaction, that then affects the crime rate. By focusing on social disorganization in cities, for example, routine activities theory was able to predict crime rates, and offer suggestions for the reduction of crime. Such daily routines as employment, recreation, educational endeavours and leisure activities were all analysed in terms of how they affected crime rates. Crime itself was analysed as requiring three components in a particular space or time: motivated offenders, suitable targets and the absence of capable guardians. Routine activities theory at first was focused mostly on predatory crime, including rape and murder but also theft or assault. According to routine activities theory, a criminal, regardless of his or her motives, chooses victims "based upon the perceived value, visibility, accessibility and inertia of the objective" (Boetig, p. 15). Technological and organizational advances in society also created new spaces in which offenders can exploit evolving routine activities to commit crime, such as highways, automobile use and telephones (it would follow, then, that the ATM machine, the Internet and other elements of electronic transmission of data would constitute a still more advanced system along the same lines). Once the offender identifies a victim, only the presence or absence of a guardian will deter the crime from happening. While usually imagined to only be a police officer or guard, it is also true that other citizens in various roles can serve as a deterrent presence that

prevents a crime from occurring. Burglar alarms, video cameras and other threats of exposure have also been found to function as guardians to prevent crime. Being in a group of people as opposed to being alone also reduces one's risk, even if the group forms without the purpose of security as part of routine activity. The presence of a handler, or a person with social control over another person, was later added to the list of factors that contributed to crime.

Derived from routine activity theory, situational crime prevention strategies were developed to combat crime, involving a careful analysis of crime situations based on routine activity. In recent years, these methods have been expanded for use in detecting white-collar crime in business environments. Routine activities theory can be applied to any crime by "collecting and examining data about the problem, describing its history, evaluating potential causes, reviewing previous interventions and identifying stakeholders and offenders" (Boetig, p. 17). To examine identity theft, then, a routine activities theory analysis would require determining the level of guardianship at sites, the suitable victims involved, what is being stolen and a profile of possible perpetrators, based on recent arrest records. This would then lead to a determination of who were the most likely culprits and the development of programs to reduce the convergence of motivated offenders with suitable targets.

In a case study provided by Boetig (2006) a rash of mid-afternoon thefts of small objects from homes around a school zeroed in on absent students: a proactive response involved working with schools to keep track of students during lunch period or after classes, improving truancy enforcement, and developing more after school programs. The handler component of the model called for the police to also become involved in encouraging community centres to create programs that exercises influence over juveniles from engaging in delinquent behaviour. Increasing basic security in the neighbourhood was also recommended, including the creation of

a neighbourhood watch. The most difficult aspect of their application of the model was reducing the suitability of the victims, which in the case of theft involves the property stolen: consumers are reluctant to reduce the suitability of their goods by buying cheaper objects (though some city dwellers do buy cheaper cars to reduce their theft suitability). Police could only warn residents not to leave these objects in open display, or within easy access. For identity theft, these models suggested that police could become involved most directly in preventing theft of personal property ranging from laptops to iphones which could result in identity theft, or of security-based bank cards or credit cards. It is strongly suggested that police would have limited ability to proactively reduce the likelihood of internet-based identity theft, as the identity of phishers is unknown, but efforts could be made to educate consumers about safer internet use. For example, an effort can be made to educate consumers online not to open any email that comes from an unsolicited source, or to not divulge personal information except in a secure website. At present, however, it would seem that experts in online security, believing in technological answers to identity theft, may not find the contribution of law enforcement to be particularly helpful. The question, based on Boetig's (2006) analysis of the application of routine activities theory to recent crime, remains open. Consumer education would also appear to be especially validated by applications of activity theory to the more micro-level behaviours of potential offenders or victims, with Smith (2009) modelling the situational cues of various locations in a detailed way. The implication of his model is that in addition to designing spaces that would prevent crime, planners must also look at who uses places and, just as importantly, who might use them if they seemed safer and also at how and when places are used (Smith, 2009).

Dunham et al. (2010) elaborated on routine activities theory to explain the role of controllers in reducing crime. They did so because the theory does not provide an explanation

for why controllers would be absent, nor does it take into consideration the role of super controllers, or those who regulate the controllers' incentives to prevent crime. Using SCP, they explored types of super controllers and the ways in which they contribute to changing controller behaviour. The controller is the handler, guardian or manager that prevents crime from happening. Handlers have emotional connections that they exploit to reduce criminal activity, guardians protect potential victims and managers smooth functioning of the place. Lack of controllers enables crime, but there is also a question as to why controllers succeed or not, and if incentives are needed to motivate controllers to engage crime, usually provided by supercontrollers. Formal, organizational, contractual, financial, regulatory, court-based, diffuse, political, market, media, personal, group and family supercontrollers are discussed, each with different ways of motivating controllers. Rational choice theory was utilized by Dunham et al. (2010) to explain how controllers can intervene in criminogenic circumstances based on effort, risk, reward, excuses and provocations. Influence is exerted by increasing penalties for controllers for not taking action, change the rewards controllers receive from providing crime prevention, manipulating excuses by introducing standards, and preventing provocative action by controllers that only make criminogenic potential worse. Overall, supercontrollers contribute to crime prevention by mobilizing controllers to engage more effectively in prevention. The importance of adding the supercontroller element to the SCP-based activity theory model is that is provides for application of the theory to many of the macro structures that constitute modern society, and this would also include the internet or sites (Dunham et al., 2010).

Farrell et al. (2010) explored the viability of routine activities theory as a possible explanation for the drop in crime rates in recent decades. Again, routine activity linked crime to socio demographic causes, and "the specific mechanism of change was the number and nature of

interactions of suitable targets and potential offenders in contexts with varying degrees of capable guardianship" (Farrell et al., p. 24). From this premise, other theories developed, such as the VIVA hypothesis, where crime is based on value, inertia, visibility and accessibility, and the CRAVED hypothesis, which measured stolen goods as concealable, removable, available, valuable, enjoyable and disposable. Environmental criminology, explaining crime according to crime pattern theory, also has much in common with routine activity theory. Farrell et al. (2010) classified all such theories as opportunity-related theories, and considered the extent to which the adoption of these theories by police departments contributed significantly to the crime drop. Namely, they questioned whether reductions in the offending or target populations and increased imprisonment contribute to the drop, or did policy in policing, ranging from zero tolerance to Compstat-based policing, contribute to the drop. They also tested if gun control, changing drug markets, increased abortion rates, stronger economies and lead exposure as a contaminant contributed.

Two hypotheses for recent crime drops were based on technological changes, resulting in some crimes being new, and others becoming obsolete, which would appear to have relevance to the internet. In reviewing these hypotheses, Farrell et al. (2010) argued that the most likely would consider both the offender and target as they contribute to criminal situations. Thus, "the set of opportunity theories incorporating routine activity theory, situational crime prevention and environmental criminology warrant far more serious considerations than they have received to date" (Farrell et al., p. 38. 2010). They then developed a concept of corporate responsibility based on these theories, which argues that companies that provide products susceptible to theft or sites of criminal activities must be held accountable for their product security gaps and be brought into corporate efforts to reduce crime. Farrell et al. (2010) specifically addressed the

role of electronics and the internet in preventing crime, and argued that the security hypothesis would help to involve all parties in reducing opportunities for crime. Thus, this hypothetical study into crime prevention specifically suggested that opportunity theories can be used to address internet-related crime.

(i) Applying Routine Activities Theory (RAT)

Fell (2006) sought to establish if there was a link between routine activities theory and identity theft victimization by examining the routine activities of college students and determining if their activities make them more susceptible to identity theft. Data was utilized from 208 undergraduate students at a southeastern university, focusing on their activities, as well as their perceptions of their own susceptibility to identity theft. The results found that how college students guard their credit card numbers and receipts has a direct impact on the likelihood of their becoming a victim of identity theft. Though recommendations were made as to increasing student awareness of identity theft and bad habits with regard to it on campus, the study did not proceed to examine if the application of this counselling program reduced the rate of victimization of students.

At the same time, it is also true that Fell's (2006) study only focused on offline student activity with credit card slips or receipts, as it might relate to routine activities theory. The relationship between routine activity theory and offline behaviour, though application of RAT to identity theft is rare, abides by the more common model on the basis of which RAT was established: criminal events on streets or in community milieu. Online environments present a different picture, which may or may not invalidate RAT. Thus, Hutchings & Hayes (2009) examined if routine activities theory explained the incidence of identity theft online measuring

the likelihood of 104 individuals in responding to phishing emails. In this case, the suitable target in an online world would be a user who was more likely to respond to a phish email, the motivated offender would be the identity theft criminal who finds phishing an easy way to obtain personal information that can then be used to access accounts, and the absence of a capable guardian, which would be a website or email server which offers little in the way of user protection against spam or phishing. The results found some confirmation for routine activities theory.

Studying user patterns of the 104 subjects, Hutchings & Hayes (2009) found that users who made much more routine use of banking websites were much more likely to be attacked by motivated offenders, bringing together offender motivation, because banking customers are dealing with money, and suitable targets, because the users are on banking sites. At the same time, Hutchings & Hayes (2009) found that heavy users of banking sites eventually become more aware of identity theft dangers and more adept at using protection, reducing the likelihood of crime. It was also found that routine email filters provided by banking sites were generally ineffective in discerning spam or phishing emails from regular emails, thus leaving the lack of guardianship an issue. By and large, however, Hutchings & Hayes (2009) felt that the study confirmed the validity of routine activities theory in explaining some degree of the likelihood of users online being victimized by identity theft offenders.

To the extent that routine activity theories in crime prevention focuses on crime in particular locales, it may well be that the coalescing of identity theft in certain sectors or locales would finally encourage entities such as banks to undertake anti-phishing efforts. For example, Bose & Leung (2009) examined the reasons for the adoption of anti-phishing efforts by Hong Kong banks. They found that while phishing scams have cost the U.S. $320 million per year, in

a figure from the year 2008, Hong Kong had become a hotspot of phishing, with Hong Kong banks being a particular target. A model was used which divided the phishing event into four phases: preparation, mass broadcast, mature and account hijack. Theoretically, preparation entails efforts by phishers to identify possibilities for phishing at banks, while the anti-phishing measures available to banks include anti-virus, auto-logoff, firewall, instruction detection system, on-screen keyboard, security team watch and encryption. Mass broadcast involves spreading the phishing with warning emails from banks being the only response. Maturity involves waiting for the victims of phishing to respond, and weapons used to prevent users from doing so include a digital server certificate and incident report hotline. Finally, account hijacking actually involves financial theft, and at present banks have account suspension, hardware devices, last logon timestamp, no simultaneous login rules, one-time password, personal digital certificate and challenge and response procedures to prevent this from happening (though several of these devices are made almost no use of). Banks are mostly concerned with phishing at the mature phase, and 87% of banks adopted digital server certificate requirements in order to stop this form of phishing. The banks did not seem concerned about mass broadcast of bogus emails from banks, but developed two-factor authentication to stop account hijacking. Bose & Leung (2009) found that small banks were better prepared against phishing than larger banks, banks with better credit ratings were more adept at security and government advocacy of a policy or procedure improved bank response (the Hong Kong government encouraged banks to institute two-factor authentication). Also, banks who had experienced more phishing attacks and the degree to which the bank participated in online banking, all influenced the extent to which a bank undertook to improve their security against phishing-based identify theft of client accounts. Bose & Leung (2009) suggested that these results were most likely relevant to banks the world over as well.

Insofar as government advocacy was found to improve bank responsiveness to phishing, the results also provide a framework for the involvement of law enforcement in advising banks, for example, on how to act more effectively in preventing identity theft online.

Routine activities theory will be operationalized in the following study by the fact that the researcher will interview all potential participants in a crime scene as theorized by the theory. That is, in terms of motivated offender, a population of offenders will be interviewed to determine what motivates them to commit a crime, how they commit the crime, and what makes it possible for them to do so, all then interpreted based on whether or not their motivation stems from an appearance of an opportunity for crime online. As far as suitable target is concerned, this study will also interview victims of internet-based identity theft to determine if in their routine activities online they created an opportunity for identity theft by failing to take necessary precautions, or lacking full knowledge of the dangers of Internet-based identity theft. Finally, guardianship as an element of a potential crime scene is examined by interviewing a number of investigators as to the most likely scenarios for online identity theft, and deriving some empirical knowledge on the most opportunistic occasions for crime. Also, their level of oversight of online identity theft, the degree to which sites and services online provide adequate protection, and the extent to which they feel the internet as a whole is able to combat hacking, and other crimes, is reviewed in relation to whether adequate guardianship exists online to act as a preventive against crime. It is expected that at present offenders will report that internet identity theft is easy, with little chance of being caught, users continue to behave online in ways that may make them an easy target and guardianship continues to be inadequate, all, according to routine activities theory, making routine activity on the internet an ideal locale for the commission of identity theft crimes.

(h) Case Studies of Successes and Failures in Law Enforcement Response to Identity Theft

It is unknown whether current methods for reducing identity theft are in fact effective. These methods will remain a matter for debate in the research. Any study which examined the response of company employees or consumers to identity theft, testing, in effect, if a program resulted in lesser number of incidents of theft, would constitute a case study on program effectiveness (Mensch & Wilkie, 2011; Ramsey & Venkatesan, 2010; Reyns, 2010). Along these lines, Mensch & Wilkie (2011) examined the degree to which one type of consumer under the aegis of one type of institution, college students attending a major university, had an awareness of identity theft, and if efforts to improve their awareness reduced incidents (Mensch & Wilkie, 2011). The research was based on previous findings that generally college student awareness of identity theft is poor. The fact that college students make considerable use of social media also puts them at risk for identity theft. Their attitudes and behaviours about identity theft, if uninformed, would only add to their vulnerability. Mensch & Wilkie (2011) argued that colleges must take a proactive approach in educating students about the dangers of identity theft, and if they do not establish formal policies student IT security practices will continue to fall through the cracks. Previous examination of student attitudes have found that students are particularly vulnerable to social engineering tactics in identity theft, which entail the perpetrator pretending to be someone other than who he or she really is. Some 64% of attacks against college students involve malware, 23% bots and zombies, 34% phishing, 29% denial of service attacks, 17% password sniffing, 11% browser exploitation and 19% financial fraud (Luo & Liao, 2007). College students are also vulnerable to spyware, shoulder surfing, dumpster diving and laptop and mobile device theft. In terms of social engineering-based fraud, 55% goes toward opening a new line of credit, 34% for stolen credit or debit cards, followed by tax and phone or utilities fraud. Some 77% of college students use social networking sites and 79% have facebook

accounts (Fogel & Nehmad, 2008; Ellison, 2007). On their profiles, 65% of students included a personal email address, 74% allowed anyone to view their profile, 10% provided a phone number, and 10% even provided their home address.

The extent to which malware can be sent through email and instant messenger services makes this finding a major concern. Mansfield-Devine (2008) showed that most college students use the same password for all of their online behaviour also means that once their social site is hacked, a hacker can proceed to other theft opportunities. Jagatic et al. (2007) study found that 72% of college students had clicked on phishing sites, with 76% of freshmen having clicked on such a site. While technology majors seemed to be aware of phishing, and clicked on such sites less than 35% of the time, other majors clicked often, with business majors clicking on phishing sites 72% of the time. Thus, Mensch & Wilkie (2011) had to question the extent to which college students behaved in a protective way online, and the extent to which they made use of security tools and updated their security software. To give their study structure, they made use of the Comprehensive Model for Information Security Systems (CIA triad) to measure student response in terms of confidentiality, integrity and availability. Confidentiality encompasses a set of rules that determines access to an account, integrity entails having assets which only authorized parties can modify, while availability ensures that data is available only to authorized persons, but available to them upon request. Awareness training was implemented to determine if it helped college students improve their awareness of the degree to which their use of the internet falls within the limits of the CIA triad model of security.

Some 2,000 undergraduates and graduates from a mid-sized university were surveyed as to their online behaviour, determining their level of security awareness and their attitudes about security online. The study found a relatively low level of security awareness among most

students, revealing, then, “a trouble disconnect (Mensch & Wilkie, 2011, p. 105). They recommended, based on the findings, that a paradigm shift is needed to get students to take online security issues more seriously. Firewalls, updated anti-virus and spyware software and pop-up blockers should be used by all students. For Mensch & Wilkie (2011), the results indicated that “a reliance on technological controls to the exclusion of people and processes is insufficient” (Mensch & Wilkie, 2011, p. 106). Thus, computer services alone cannot prevent identity theft; users must be trained in awareness, to promote sound behavioural practices, in order to protect the CIA triad elements of their data. Awareness training should include social engineering awareness, risks of file sharing, risks of unknown websites, the risk of clicking on unknown emails, the importance of regular data backups and the importance of security updates. Users should also be trained in strong password construction techniques (best are 8 characters or longer, combination of letters and numbers and mixed upper and lower case), password management techniques (change passwords often, use different passwords for each account, do not share passwords, use mnemonics to remember passwords, etc), phishing configuration detection methods and institutional level security policy compliance.

While training is important, studies have also found that students who have received training still engaged in risky online behaviour. One study of West Point cadets, for example, found that 80% of them were still clicking on phishing sites after training, and the lure of social media often makes college students prey to ever more sophisticated methods of theft (Ferguson, 2005). Nonetheless, the importance of Mensch & Wilkie’s (2011) findings was that they provided support for the notion that the human factor is the major weak spot in identity theft prevention, especially online, and that the people factor must be addressed alongside of technological fixes in order to prevent more identity theft from occurring. That is, “people and

systems must work together to minimize vulnerabilities" (Mensch & Wilkie, 2011, p. 108). Insofar as this paradigm change attempts to train individuals to protect themselves from identity theft by altering their routine behaviour online, and by putting in place a higher level of institutional guardianship to watch over them, it is easy to see where consultation with law enforcement to provide training models built on routine activity theory and the situational crime prevention framework would correlate almost point for point with such programs. While Mensch & Wilkie (2011) did not mention law enforcement as part of the consultancy equation in either college creation of security policy or in actual training of students to be more aware of the dangers of the Internet it is entirely foreseeable that at this intersection law enforcement and technology experts could again collaborate to reduce identity theft crime, even by online means, not by creating a technological response, but by removing the opportunity provided for crime by the unaware routine activity of college students online.

While research has called for partnering of platform-based private enforcement actions, usually of a technical nature, and law enforcement, in order to deter and prevent cybercrime including identity theft, a major stumbling block in applying a theoretical crime prevention approach to the Internet has been that the internet is unlike any space where crime has taken place previously (Reyns, 2010). In the case of the situational crime prevention model of combating crime, for example, the question with regard to the internet is: what is the situation, what is the context? Therefore, research is required which seeks to apply law enforcement paradigms to combat crime online, in order to develop this paradigm. While not focused directly on the cybercrime of identity theft (examining, in fact, cyberstalking), this is precisely what Reyns (2010) attempted to achieve in his study of how the situational crime prevention paradigm could be utilized to combat this form of cybercrime. Cyberstalking involves stalking through the

various means of emails, instant messaging, blog posts, text messages and other annoying and persistent communications. How to deal with cyberstalking remains a question, because for many it remains unclear what it is, and it is a very new crime. In proposing a preventive approach to this cybercrime which focused on limiting the opportunities for cyberstalking, Reyns (2010) argued that "the techniques of situational crime prevention are ideal for this task" (Reyns, 2010, p. 99). He undertook his study without a firm research basis, acknowledging that "the scarcity of criminological and victimological theory as they relate to cybercrimes makes it difficult to identify risk factors for cyberstalking victimization" (Reyns, 2010, p. 99). Therefore, the situational crime prevention framework, including both opportunity and routine activity theory, must be tailored to online contexts, even as the concept of place management "makes a fairly straightforward transition from an offline to an online setting" (Reyns, 2010, p. 100). Reyns (2010) also argued that the techniques of the SCP paradigm, including, as noted before, increasing the effort, increasing the risks, reducing the rewards and removing excuses, seem applicable to online contexts. The notion of opportunity structures, involving intimate, acquaintance or stranger relations between email correspondents, also applies. This then would apply to preventive measures, as, for example, it has been found that persons who post less personal information online are less likely to be subject to cyberstalking.

Reyns (2010) examined cyberstalking and found that at present it is estimated that 14 in every 1000 persons older than 18 have been cyberstalked and that females who were stalked received emails as part of the harassment campaign 24.7% of the time. To apply SCP to cyberstalking, Reyns (2010) recommended considering any place online where motivated offenders and suitable targets converge as a potential site for the crime. He recommended that blog sites, social networking sites, chat rooms, email services and group pages all be thought of

as places just as street corners would be conventionally viewed in offline application of SCP. Efforts would then be made to make these places less hospitable for crime. This entails the application of routine activities theory which as noted conceptualizes a crime opportunity as consisting of a suitable target, motivated offender and lack of capable guardian. Applying this model, website managers would be the guardians, and thus have an important role to play in the prevention of cyberstalking. These managers can control what happens on their sites to prevent crimes; especially as computing itself is primarily a solitary activity. They can do this by focusing on the so-called criminogenic properties of websites characterized by one researcher under the SCAREM rubric, entailing, that is, stealth, challenges, anonymity, reconnaissance, escape and multiplicity. That is, the online environment allows for invisibility, provides an enticing challenge to hackers, protects their anonymity, enables scanning for opportunities, makes avoiding detection easy and provides multiple targets. Social networking sites are particularly criminogenic in these terms.

It is also true that information is what is called in criminology a hot product or something likely to be taken by offenders. According to the aforementioned CRAVED model, a hot product is stolen because it is concealable, removable, available, valuable, enjoyable and disposable. Credit cards, cell phones, ipods, etc., all share CRAVED characteristics. Personal information online is no different. With these rubrics in mind, SCP seeks to reduce opportunities by analysing and manipulating the mechanisms which create opportunities for crime. By altering the physical environment, they can be reduced. By breaking down large problems into small problems, the environment of opportunity for crime is gradually diminished. Using specific crime-prevention methods, in this case applied specifically to the characteristics of cyberstalking, and by offering crime-situation specific solutions based on understanding how the crime is

committed, SCP can be applied. These methods again focus on increasing the effort, increasing the risk and reducing rewards.

Online, the exposure of victims to the opportunity of cyberstalking is a major problem, and SCP would work to reduce this exposure. This could be done by means of changing the lifestyle exposure of online users, meaning that users would be trained to provide less information, stay anonymous, not reveal their gender, use only first names, not reveal their age and guard their credit card information. Cyberstalking is also activated by repeated attempts at communication: disrupting the ability of the offender to communicate would curtail this situation, primarily through the web master, acting as guardian, providing filters to filter out unwanted communications. Use of email by cyberstalkers could be reduced if users are trained to not email back unknown parties and website managers increase efforts required to email addresses to members. Managers could also embed spam filters in all site communication, and warn users never to reply to a cyberstalker. With blogging, the web master could monitor public blogs for misuse while the user could limit access to their accounts. This same combination of preventing user response to unknown communication and web manager erection of difficulties to such communication on the site in general will apply SCP to the online environment in ways that reduce crime.

Reyns (2010) acknowledged that the most difficult aspect of SCP to apply to online context is reducing provocations; as it is not yet theoretically clear why cyberstalkers engage in stalking in cyber environments. Avoiding disputes and reducing emotional arousal appear to be best means to reduce opportunities. It is possible that when a user provides continual updates to an unknown source he or she feeds the fire of the stalker, thus, this behaviour should be curtailed. Never replying to inquiries could also prevent the stalker from gaining a sense of control over the

relationship, believed by many to be one of the motivations for stalking. Finally, removing excuses, which involves setting rules and posting instructions, should be built into agreement to participate on a site. Constant reminders from the web managers on how users should address unknown inquiries have been found to reduce crime. Thus, Reyns (2010) applied the concept of place management to online environments and found a strong degree of fit between SCP strategies used in real space and virtual space. Reyns (2010) also entertained the notion that controllers and supercontrollers, or those who enable the controllers, contribute significantly to crime reduction. In the online environment, super controllers would include those who make decisions regarding web protocol. While conceding that this was uncharted territory in the crime prevention literature, and not conducting a case study of an application of the SCP model to the prevention of cyberstalking (his study being an exercise in model building and paradigm changing), this study nonetheless provided a bridge in applying a law enforcement paradigm to prevention of cybercrime, presumably including identity theft.

Zaharia et al. (2010) applied routine activities theory to the internet, seeing the internet as a challenge to the model, insofar as the way in which motivated offenders and suitable targets converge on the internet is different than in real space. Nonetheless, studies have shown that socio demographic factors shape routine online activity, and that these factors combined with activity can mediate the likelihood of being targeted online. As a result, Zaharia et al. (2010) argued that situational crime prevention theory provides a useful framework for limiting opportunities for victimization on the web. Because the internet has increased the opportunity for crime and the type of criminal activity that can be committed, it would follow that a prevention theory based on limiting opportunity would be an effective approach to prevention. At present, Zaharia et al. (2010) argued that transparency online is the best way to prevent

identity theft in the conduct of an electronic market, using the SCP to propose ways to ensure that crime does not result from routine participation in such markets. Wortley & Mazerole (2008) supports RAT as it relates to prevention by increased risks of detection and apprehension. This applied RAT is likely to have a positive effect in deterring identity theft.

Ramsey & Venkatesan (2010) appeared to view cybercrime as a crime of opportunity enabled by the fact that due to social media and online shopping more online applications are storing confidential and valuable user information. That is, a newly routine behaviour of accessing internet entities has created new opportunities for cybercriminals. To reduce this crime, Ramsey & Venkatesan (2010) also proposed a primarily preventive approach which would remove these opportunities for crime. They proposed the proactive development of an integrated anti-cybercrime framework which explicit employers use for education, technological measures, private legal enforcement, and "partnerships with law enforcement" to prevent and deter identity theft based on opportunities provided by the Internet (Ramsey & Venkatesan, 2010. p. 23). As such, they closed the gaps that continue to plague the research into rules and standards to prevent identity theft online. They focused their study not on theft directly from users, through such means as phishing, but on the fact that "between 12 percent and 27 percent of identity theft occurs from data breaches at third party companies that hold or control user information" (Ramsey & Venkatesan, 2010. p. 23).

With viruses against this sort of storage doubling per year since 2006, and the development of a rapidly expanding underground of hackers, including the use of botnets, or compromised computers that deliver malicious software, occurring at a global scale, a more comprehensive preventive approach is needed. Again, Ramsey & Venkatesan (2010) argued that social networking and the overall trend toward cloud computing, where users store information

on remote servers, have created new and attractive opportunities for cybercriminals to engage in identity theft. The fact that so many users are on social media sites makes it profitable for phishers to attack these sites as even gaining a very small proportion of response can lead to great profits. The fact that social networks are mass media built on trust-based architectures, connecting users based on pre-existing personal connections, means that this trust can be abused by phishers. Studies have found that users are more likely to trust spam sent in the context of a social network than elsewhere in general email, resulting in more breaches. Romance scams, where cybercriminals approach users feigning a romantic interest, to obtain information or money, are also on the rise, also exploiting trust. Automated cyberattacks also work much more effectively on social sites, posting invites to events that only download Trojan viruses. Due to all of this new opportunity, then, specifically indicated by new online contexts, cybercrime has increased six-fold over the last two years.

Linked to this, Ramsey & Venkatesan (2010) reviewed three different models of addressing cybercrime: user education and self-help, private enforcement and partnerships with law enforcement, focusing on evaluating their effectiveness. Some social sites offer user education services, such as security blogs informing users about problems, tutorials in best practice and security pages that release user self-help applications to users. Cloud computing sites offer similar services, including how-to resources on malware detection and prevention. Ramsey & Venkatesan (2010) found that while self-help and user education approaches are helpful, they cannot stand alone in response to cybercrime insofar as they do not threaten cybercriminals with any consequences, and as such have no deterrence function. It is also true that new cyberattacks can occur quickly and without warning, meaning that user education often happens after the fact, or after users have already been victimized. Legal recourse against

cybercrime is the second model made most use of by sites, but there are many legal challenges to this process that currently makes it less than effective. By contrast, the second type of prevention used by sites entails private enforcement efforts. These efforts are defined as those undertaken by sites against cybercriminals in the form of attacks on the technical infrastructure which supports cyberattacks, targeting nodes in a coordinated attack, and engaging in organized cease and desist attacks. An example is provided by Ramsey & Venkatesan (2010) of a cloud company that dismantled a botnet by taking down several hundred domains that enabled the botnets to communicate. Another example would be when the FTC shut down a net hosting company that was found to enable misconduct by users. All of these efforts are helpful to the extent that they can add to cybercriminals' operating costs and put added pressure on them to stop their activity. When the disruptive approach fails, however, platform owners can then bring legal actions against spammers and fraudsters to disrupt and deter their activities. The main problem with the private enforcement action paradigm is that it requires platform owners to quickly develop a sense of the architecture of cyberattacks, that is, the online context which enables the attacks, and given the spread out and geographically dispersed nature of the internet, this can be quite difficult. While tools exist to identify hackers, moreover, and social networking sites may have the tracking infrastructure to do so, the proactive development of these architectures may be a challenge. Nonetheless, Ramsey & Venkatesan (2010) did not rule out the potential effectiveness of these private enforcement methods involving, essentially, engaging in cyber war, weapon against weapon, against cybercriminals.

Finally, the third model for combating cybercrime is partnering with law enforcement. This approach has been enabled by the fact that federal law has criminalized many cybercriminal activities ranging from spam to theft, often supported by other state laws. Criminal prosecution

undertaken through the state attorneys general or public consumer protection agencies to bring civil suits against sites or platforms supporting crime have been effective. Partnering with law enforcement is also cheaper than privately prosecuting criminals. A number of case studies have emerged of successful civil legal attempts to shut down cybercriminals. In one case, a hacker was sentenced to 20 years in prison, and the so-called Godfather of Spam also received four years in prison for violation of federal law. Another advantage of partnering with law enforcement is that jurisdictions often already have in place multilateral assistance treaties and law enforcement agencies generally have broader legal tools with which to work against cybercrime. At the same time, whether or not law enforcement has the manpower or time to engage in pursuit of cybercrime remains a problem. It is also critical that platform owners collect material technical information on cyberattacks which can be used in a court of law, and others have raised concerns about sharing of information with law enforcement as well. Finally, criminal prosecution as opposed to private-originating civil action takes more time, and can often interfere with the latter.

As with researchers who argued that standards are more effective than rules for combating identity theft online, Ramsey & Venkatesan (2010) appeared to echo the notion that the broader legal tools which law enforcement has as its disposal for attacking identity theft online would be a major reason why partnering between platform owners and law enforcement would be recommended. Overall, however, Ramsey & Venkatesan (2010) concluded that the best way for any progress to be made against identity theft in its online form is to fashion partnerships between platform private enforcement, legal action and law enforcement and prosecution. As a result, Ramsey & Venkatesan (2010) established that emerging best practice in combating identity theft may supersede the technological warfare private enforcement model, as

well as the legal model, and have to encompass law enforcement, using methods based on the situational crime prevention model, in deterring identity theft. Proof that application of emphasis on guardianship, according to routine activity theory, can reduce crime was found in a survey of victim behaviour after theft (Haywood, 2007; Conradt, 2011). Widespread change of behaviour was found, including document shredding, not opening unsolicited email and monthly review of bank statements. Thus, victim preventive behaviour surpassed the average users' behaviour.

Berg (2006) undertook a survey of the quality of the instruments utilized at present to measure the extent of ID theft. It was found that current identity theft victim profiles need to be enhanced, the methodologies used in identity theft surveys are suspect, and current identity theft survey instruments have deficiencies. Telephone surveys are becoming increasingly suspect with the public changing over from landlines to cell phones. The fact that most surveys continue to be undertaken only in English also limits data accuracy. The fact that only adults over the age of 18 are surveyed is also a problem, with many respondents over 18 also missed because surveys only address one person per household. Berg (2006) recommended changes that entailed, focusing more on age and gender of victims, ensuring that respondents know the meaning of technical terms, fully explaining the preventive measures that can be used against identity theft. In this regard, Berg (2006) commented "while support remains limited for routine activities theory tied to high tech crime, and specifically identity theft victimization, it is nonetheless important to recognise that engaging in certain online behaviours may make an individual more prone to becoming a victim" (p. 52). Engaging in online gambling, answering unsolicited emails, linking to sites indirectly, viewing online pornography, have all been found to be "routine activities" that make users more susceptible to identity theft. Even surfing the web with abandon, going to unknown web sites, increases the odds of having a computer spyware attached to one's browser.

Online chatting also opens one up to virus infection. In response to this behaviour, then, Berg (2006) called for preventive behaviour programs, in accordance with routine activity theory.

With regard to the best way to prevent identity theft, either off- or online, Copes & Vieraitis (2007) found that a number of situational crime prevention techniques may be helpful, but may become less effective as methods of crime commission online become more sophisticated. At present, Copes & Vieraitis (2007) recommended that controlling access to business and residential mailboxes and dumpsters, having companies and individuals monitor how they dispose of documents, including more shredding of documents, limiting the number of employees who have access to sensitive information in all companies, and conducting background checks of all employees employed by a company. On a broader level, creating a positive work environment may forestall negative employee activity like stealing personal information. With regard to banks, Copes & Vieraitis (2007) recommended that passwords be required even for in person transactions, and training bank employees in recognising customer behaviours indicative of dishonest activity. As for stores, consistency in checking personal identification must be established. All of these methods, removing opportunity from criminal contexts due to strengthening of guardianship, abide by situational routine activity theory crime prevention. At the same time, Copes & Vieraitis (2007) recommended that identifying fraudsters' use of excuses enabling them to commit the crime be foreclosed upon by educating all employees to the consequences of identity theft and placing messages in banks or stores reminding offenders that identity theft crime has real victims.

(i) Conclusion

This review found a dramatic increase in identity theft over the past five years, and a quickly evolving, and ever worsening scenario in terms of crime growth. Because identity theft

is a relatively new crime, the research appears to remain in a reactive mode against hackers who are coming up with ever more sophisticated ways to steal identities. This situation has grown worse in the last few years because of the relocation of the bulk of identity theft to the internet, where the growth in online shopping and social networking has created an under-protected opportunity for identity theft (Bronk, 2008; Giles, 2010). The review then examined the various approaches for combating identity theft, finding that while the legislative approach has focused on notification of breach laws, and imposing red flag rules for companies to self-regulate their own handling of sensitive personal data (Curtis, 2011; Domonell, 2011), industries have drawn up standards of compliance which would be a prerequisite of doing business in an industry, while information scientists continue to remain locked in a high-tech game of internet-based warfare, persisting in the belief that there is a technological solution to identity theft (Burdon, 2011; Coats, 2008; Glithero, 2009; Winn, 2010).

By and large, however, a strong undercurrent of a common preventive and consumer awareness education theme was found in the research literature in all areas. This language then echoed strongly when the review considered the extent to which law enforcement can help in the response to identity theft, especially on the internet. While police response to laptop theft or credit card theft, or the theft of identity due to muggings at ATMs would seem obvious, how the police respond to internet-based identity theft remains a problem. The theoretical situational crime prevention model, including routine activities theory, provided a model for policing against theft, and upon review the language of prevention, with a focus on consumer awareness built into the model, sounded similar to recommended responses by experts in the field (Miethe & Sousa, 2010; Tillyer & Kennedy, 2008). That is, it would appear that even technical experts have begun to see that changing the culture of the internet in terms of reducing opportunity for

crime, educating consumers to be more aware of identity theft crime, and empowering controllers and supercontrollers, as in the case of industry standards, would reduce crime more aggressively than strictly red flag or technological solutions. The review concluded with a few case studies of the effectiveness of the situational crime preventive paradigm, applied explicitly, though as yet only in model-building exercises, to instances of internet crime (Mensch & Wilkie, 2011; Ramsey & Venkatesan, 2010; Reyns, 2010). While these studies did not test the model on actual incidence of internet crime, the research demonstrated that the situational crime prevention model applied to identity theft would do a great deal to help reduce crime, and involve law enforcement, through consultancy, consumer education and assistance in self-policing, in a direct way in combating identity theft whether it originates from crime on the street or on the world wide web.

CHAPTER 3: The Research Methodology

(a) Introduction

This chapter will present the research methodology and design developed for this project. The design was chosen based on the original motivation for undertaking the project, based on the researcher's experience as a detective, assigned to the Manhattan District Attorney's Office for seventeen years, namely, that insofar as identity theft continued to grow, while law enforcement response did not, a better grasp of the scope and scale of the crime was required in order to promote an effect to close the gap between crime and prevention. The design of the research project, primarily based on interviews, evolved out of the significant portion of the time devoted to criminal investigation during the researcher's tenure in the Manhattan District Attorney's Office Detective Squad focused on white-collar crime, including identity theft. For this reason, the professional experience of the researcher formed the basis for much of the insight provided in this study into the problem of identity theft, combined with research and data gathering from the field through interviews with key stakeholders.

(i) Research Methodology and Design

The personal involvement of the researcher in the field under study in this research project is the basis of the research design. As a result of the depth of involvement in identity theft or fraud investigation, my level of knowledge, according to Hammersley and Atkinson's Ethnography Principles and Practices scale of levels of involvement, would be classified as complete participation. That is, as a detective focused on white-collar identity theft crime my career included active involvement within the culture of white collar crime, fashioning a network

of contacts and colleagues who supported my work, facilitated by inter agency meetings, coming in contact with offenders or victims of identity theft in person or by phone and frequently travelling to foreign countries for the purpose of coordinating our investigation with those of international agencies such as Interpol, often with the intention of extraditing apprehended criminals back to the U.S. for prosecution. In this way, my work became highly specialized, and, involved interacting with colleagues with an equal interest in identity theft, thereby developing a culture within criminal investigation focused on the particulars of this kind of crime, somewhat in opposition to the mainstream operations of the District Attorney's Office. Many of the insights gleaned from this culture form the ethnographic basis of my investigation.

Having accrued a significant number of years of experience in the investigation of identity theft, my concern about the serious nature of the crime and the general lack of attention of police departments to the crime coalesced into a few key research questions which it is the purpose of this research to answer. Therefore, this research project was launched. This study involves two primary sources of data. First, a series of interviews with investigators, police officials, industry stakeholders, lawmakers, prosecutors, fraudulent individuals and victims of identity theft were conducted. Originally, these interviews were conducted as a routine part of ongoing investigations, but in this study an increased focus on this research project led to a more formal collection of data from interviews. Second, this body of knowledge was then expanded and deepened by a complete review of the research literature into identity theft and fraud and its impact on U.S. society today, as well as by examination of the primary documentation of recent legislation passed to combat identity theft as well as police records, to obtain a full sense of the dimension of the crime. The purpose of the review of the literature as well as the review of

legislation was to determine the extent to which laws and law enforcement mechanisms are in place to address the problem of the rapid expansion of identity theft.

Therefore, the research base for this study is composed of three data sets: first, knowledge accrued from my professional experience as an investigator with the District Attorney's Office into identity theft crime, as well as my attempt, in this research, to gain access to departmental records regarding the extent and seriousness of identity theft; second, a literature review of the research into the importance of identity theft both in research and government publications; and third, informal and formal interviews with investigator specialists in identity theft, law enforcement and criminal justice officials generally, as well as industry stakeholders, identity theft offenders and identity theft victims. On the basis of this research, this study was conducted.

In all stages of this study, obstacles to the study of identity theft were encountered. With regard to my professional work in investigating identity theft, numerous bureaucratic obstacles to full investigation and prosecution of identity theft were routinely encountered. Not only was the general attitude of the District Attorney's Office and police department characterized by a laissez-faire attitude about this kind of crime, but identity theft was not given priority, few seemed aware of its growing prevalence, and few mechanisms were in place with which to prosecute it. Lack of adequate response not only caused investigators focusing on identity theft into a distinct culture within the law enforcement community, but forced us, in our routine work, to have to champion the cause of identity theft criminal prosecution as well to prosecute it.

In the first part of the project, as part of my professional experience in identity theft investigation, the data collection processes of police departments and the criminal justice system in general were examined. A review of the data sources, when compared with my knowledge of

the extent of identity theft crime, indicated that current methods of data collection on identity theft are inadequate, and in need have reform. This would entail both improving the level of statistical analysis applied to the data, but developing inter agency cooperation to improve the collection and analysis of identity theft data. This phase of the research left me with serious questions about the current reliability of the data collected by the criminal justice system on identity theft. To meet the requirements of data collection for a doctoral study, several sources were assessed, including field studies and surveys. A review of existing data collection systems on identity theft in the criminal justice system found that present capabilities leave much to be desired. The research into data collection methods found that no law enforcement agency at present utilizes a central repository of data to either record instances of identity theft or to monitor the development of the crime, in terms of numbers of crimes. The ad hoc data system currently in use by the New York City Police Department is typical of the systems in place. Though it is hoped that the current system will provide sufficient data for the police department to devise an enforcement strategy for this particular kind of crime, especially in light of its rapid escalation in recent years, the current ad hoc system, in my view, does not form an adequate basis for doing so. This conclusion was made as a result of an empirical study of the current data collection system, which found that statistical information was often lacking, and the data currently in the system lacked validity.

The second part of my research project began when, based on my appraisal of the inadequacy of departmental data collection regarding identity theft, a need arose to derive more authentic, empirically-based data on identity theft. Interviews with persons directly involved in identity theft, or its prosecution, were required, and these interviews were conducted.

(ii) Consent for Research

Before pursuing this part of the research project, it was necessary to gain consent from the District Attorney's Office, the police departments in which the interviewees were either, if investigators or officials, employed, or, if offenders or victims, processed. This was done by submitting a full description of the project, its research questions and assurances of the ethics, including the protection of confidentiality to all non-offenders involved in the project. My official assignment enabled me to conduct interviews with professionals within the criminal justice system and its ancillary support units, the general public, and victims of identity theft. How local, state, federal and international governments share information was also revealed. My assignment exposed me to various facets of identity theft. After Cardiff University granted me permission to undertake this study, it became clear that it was not possible for me to continue to handle cases as an investigator working on "routine" investigations and at the same time situate myself as an objective researcher. As such, after meeting with him, the Manhattan District Attorney, Robert Morgenthau provided me with a verbal commitment from him to investigate more complex cases while conducting this study. This also resulted in being awarded a promotion and subsequent assignment to investigate high-dollar cases, broadening the potential for my exposure to 'big picture' data as the extent and seriousness of identity theft crime as handled by the department and office.

(b) Participants

(i) Inentity Theft Investigators

The first group of interviewees was a select number of fellow investigators specializing in identity theft fraud. The purpose of these interviews was to gain a sense of their perception of

the adequacy of identity theft investigation. Twenty five investigators in 7 offices and 7 departments or jurisdictions in the U.S. were interviewed. All of these interviewees were known to me from professional contact or collaboration. The identities of these interviewees were kept confidential in order to protect their confidentiality, in addition to facilitating their openness in expressing their perceptions and opinions about the current state of identity theft investigation.

The primary sources of identity theft data utilized in this research were generated from field observations at the Manhattan District Attorney's Office, Identity Theft and Cyber-Crimes Bureau, located in the Supreme and Criminal Courts building in lower Manhattan; The New York City Police Department's Identity Theft Unit, located at a training facility in Brooklyn; A United States Postal Facility, located in the Whitestone area of Queens; The United States Secret Service Office, located in Brooklyn ,New York; and the New York City Police Department's, Manhattan South Grand Larceny Task-Force, located in the Midtown area of Manhattan.

(ii) Officials

The second group of interviewees consisted of higher-ranking officials in the District Attorney's Office and in various police departments, who were purposely chosen because they were not specialists in identity theft or fraud investigation. This strategy was adopted in order to gain a sense of the general attitudes of key actors in the criminal justice system with regard to identity theft. Additionally, more than twenty five interviews were conducted with law enforcement officials and attorneys from the Kings, Nassau, Westchester, Richmond County, along with Chicago's, Cook County District Attorney's Offices. Officials from New York and New Jersey Attorney General's Offices also provided information. The names of these interviewees were anonymized to protect their confidentiality.

Overall, several hundred personnel in the criminal justice field were interviewed, including police personnel, prosecutors, judges, and college professors, investigators from the credit card and financial industry, and fraud prevention individuals from the National Retail Federation via the telephone and while attending meetings and conferences. There were no preparations for scheduled interviews and the responses were ethnographic. All participants were told that they would be notified of the results of this study. It may be unrealistic to contact every individual who took part in the study but every attempt will be made to contact them and offer my heartfelt thanks for their valuable assistance. Such contacts will also refer participants to a synopsis of key findings that will be placed on the internet upon completion of the study.

(iii) Offenders

Twenty-five offenders (25) were chosen to participate in the research, based on the fact that they formed a cross section sample of the hundreds of individuals interviewed as part of my work over seventeen years. Some of these twenty-five persons were identified as a result of observation of their courtroom trials. Others were identified by asking Central Booking personnel or inquiring from arresting officers if any of their arrests over a given period of time were for identity theft crimes. Contact was subsequently made to discuss the possibility of an interview, and arrangements made to arrange for an interview at a mutually agreed upon location. The interviews took place at different times and places in the process of their case. Some were interviewed during prisoner transport, after they were released from custody, or after the process of their case. Interviews were conducted at the District Attorney's Office, at restaurants and even on the street. Offenders originated from the United States, Mexico, the Dominican Republic, Jamaica, Haiti, Russia, Yugoslavia and Moldova. A majority had served prison terms and some

were only fined or placed on probation. However, in this study, all offenders will be referred by anonymous names.

(iv) Victims

Twenty-five victims (25) of identity theft or fraud were also selected from a wide selection of potential victims. These too were chosen based on identifying them through observation of courtroom trials. Others were also identified by inquiring of arresting officers as to their identity. Contact was subsequently made to discuss the possibility of an interview, and arrangements made for an interview at a mutually agreed upon location. Here, too, interviews took place in numerous venues. Sources at four large retail stores were helpful in providing information, specifically, pedigree information on victims as well as methods used by fraudulent individuals in perpetrating their crimes. Information was also compiled on illicit addresses used by the fraudulent individuals, along with victim's information for those addresses. In this case, however, the identities of the victims of identity theft were kept confidential. A further attempt was made to enquire about the characteristics of the victims. Of the 25 victims who participated in this study, 15 agreed to provide that information which is illustrated below in table 1. The 25 victims who were interviewed answered questions relating to 10 areas of identity theft. Those responses to the questions are shown in table 2 which is immediately following table 1.

Victims Response to Questions on Characteristics

TABLE 1

Victim #	State/Country of Residence	M/F	Age	Race	Status	Occupation	Education
1	Australia	M	67	W	M	Retired	College

Victim #	State/Country of Residence	M/F	Age	Race	Status	Occupation	Education
2	Washington	F	44	W	S	State Dept.	PhD
3	New York	F	39	B	D	Trader	JD
4	New York	M	19	H	M	Securities	College
5	Nepal	F	58	A	mm	Merchant	High School
6	China	F	23	A	S	Student	College
7	Barbados	F	38	B	M	U.N.	College
8	Argentina	M	38	H	S	Undocumented	Elementary
9	Ghana	F	25	B	M	Unemployed	High School
10	New York	F	60	W	M	Retired	High School
11	New York	Other	54	B	S	Nurse	College
12	Ohio	M	29	W	S	Plumber	High School
13	New Jersey	F	40	W	M	Teacher	College
14	Israel	M	46	W	D	Jeweler	High School
15	Florida	F	50	B	D	Unemployed	Some College

Note: Some nationalities, occupations and additional information of those victims who were interviewed are listed in the above table (table 1).

The following table (table 2) shows the results from 25 victims who were interviewed.

The questions are displayed in Appendix 3 and are as follows:

During the last two years have you or anyone you know discovered that someone:

Victim's questionnaire - Response to Questions 1 through 10 as shown in Appendix 2

TABLE 2

Victim #	Used or attempted to use credit cards or credit card information without permission?	Used or attempted to use any other existing account (s) other such as bank accounts or debit cards, or checks, without the account holder's permission?	Used or attempted to use personal informatio n to obtain new loans, incur debts, open other accounts, or to commit other crimes?	Did these actions occur separately or simultane ously?	Which incident of identity theft was quickly discovered?	How did you become aware of the theft?	What was the total dollar amount of the theft?	Have the misuse of the various account(s), forced you, a family member, or friend to close any accounts?	How much time did you spend clearing up your record?	Have you or anyone you know had utilities cut off, been a subject in a criminal investigation, gotten physically hurt, or forced to close accounts because of misuse?
1	Y	Y	Y	Sep.	Credit	DC	$250.000	Y	On	Y-Co
2	Y	Y	Y	Si.	Credit	FI	$500.000	Y	On	Y-Co
3	Y	N	Y	UnK	Auto	Police	$90.000	Y	13 Mts.	Y-Co
4	Y	N	Y	Sep.	Credit	Mail	None	N	N/A	N
5	Y	Y	Y	Si.	Credit	Lawyer	$1.5 mil.	N	On	Y
6	N	N	Y	Sep.	Phone	Police	UNK.	N	On	Y
7	Y	Y	Y	Si.	Credit	Police	None	N	On	Y
8	Y	N	Y	Sep.	Credit	Police	UNK.	Y	On	N
9	N	N	Y	Sep.	Mail	Police	None	N	On	Y
10	Y	Y	Y	Si.	Credit	Police	$45.000	Y	On	Y
11	N	Y	Y	Sep.	Internet	DC	$147.000	Y	3 Yrs	Y
12	N	Y	Y	Sep.	Mail	DC	$24.000	Y	On	Y
13	Y	Y	Y	Sep	Mail	FI	None	Y	6 1/2 yrs	N
14	Y	N	Y	Si.	Credit	Lawyer	UNK	Y	7 Yrs	Y
15	Y	N	Y	Si.	Credit	FI	UNK	Y	1 Year	Y
16	Y	Y	Y	Si.	Mail	DC	None	Y	On	Y
17	Y	Y	Y	Sep	Mail	Police	$10.000	Y	16 Mts.	Y
18	N	Y	Y	Sep	Phone	Police	$22.000	Y	27 Mts.	Y
19	N	Y	Y	Si	Credit	DC	$300.000	Y	On	Y
20	Y	Y	Y	Sep.	Credit	Mail	$925.000	Y	On	Y
21	N	N	Y	Sep.	Credit	FI	$14,000	Y	4 Yrs.	Y
22	Y	Y	Y	Si.	Mail	Police	$600.000	Y	9 Yrs.	Y
23	Y	Y	Y	Si.	Mail	DC	$479.000	Y	8 yrs	Y
24	N	Y	Y	Si.	Mail	Mail	$2.3 mil.	Y	On	Y
25	N	Y	Y	Sep.	Mail	Police	$850.000	Y	On	Y

(c) Secondary Data Analysis

The first part of my research entailed obtaining extensive documentation on the state of the art in terms of identity theft criminal justice system response and investigation. A substantial amount of information was gleaned from current and past issues of electronic periodicals and publications from the library at Cardiff University. Over 100 articles and pieces of information were collected from newspapers throughout the United States, mainly from The New York Times, The Wall Street Journal and The Law Journal. Some web sites on the Internet, such as, the Federal Trade Commission, the United States Department of Justice and Javelin Strategy and Research also provided vital information towards this research.

Some data for this study derives from reports, crime records and publications done by entities such as, the New York Police Department Identity Theft Unit. Identity theft data from contemporaries had already been established as vital associates of mine during the course of my official duties was obtained. Additional data was found in libraries such as the John Jay College of Criminal Justice and in other City Universities in New York (CUNY) libraries. A dozen books were retrieved (Hayward 2004, Sparrow 1996, Richards 1960, Van Duyn 1985, Taylor 1999, Collins 2006, Hammond) relative to identity theft. Some of these publications did not portray a contemporary status of the problem and offered very limited empirical research into identity theft. Two volumes of *Fraud: Organization, Motivation and Control* were more comprehensive, and assisted me in my research experience (Levi, 1999). Additional sources issued by agencies of the federal government, as well as accounts from convicted fraudulent individuals were also reviewed. Victims who had been scammed in cases of identity fraud also provided data.

Raw data on identity theft was derived from sixty- two law enforcement files containing the following information:

Military time and date of the report.

Arrest/Complaint number.

Arresting officer's department, command, identification and shield number.

Arrest information, time date, location, Property Clerk's Invoice number (voucher) – Fleet Visa card bearing number 432630000.....

Name of defendant (identity thief), their New York State and FBI identification numbers, including all AKA's (also known as) - (nick names).

Their date of birth, sex, ethnicity, telephone number, clothing worn, special body marks (tattoos, scars etc.).

Charges – e.g. Identity theft, grand larceny, forgery, criminal possession of stolen property and possession of a forged instrument.

Narrative-e.g. At time/place/occurrence (T/P/O) defendant did use forged credit card to obtain merchandise in excess of $1000, 00. Defendant was also in possession of another forged card.

Crime incident data – Action towards victim, method of transportation.

Sworn affidavit, with narrative signed by arresting officer.

Officer's notes, photos, handwritten confession.

Contact information at Credit Card Company.

Time elapsed between the crime and the arrest.

The number/name of additional defendants or criminal groups to which they belong.

The total loss by victim or entity

The penalty the identity thieves received and sentencing date.

Despite difficulty in acquiring data from the United States Attorney's office, other interested parties granted me limited access to twenty two files that dealt with important data involving identity breaches and large-scale money losses.

(i) Statistical Reporting

There are no absolute statistics on identity theft. The Federal Trade Commission (FTC) is the main entity for compiling statistics, although there are several other entities such as the Bureau of Justice that purport to track complaints. However, law enforcement statistics are often not shared or divulged to other groups. Furthermore, not every victim reports the crime to law enforcement. Therefore, the reporting system is systematically flawed. An FTC (2011) report showed that during calendar year 2008, 2009 and 2010, 64%, 27% and 28% of victims failed to report incidents of identity theft to law enforcement. In the U.S., we believe identity theft losses incurred by financial institutions to be staggering; however there are no clearly defined figures.

Congressional hearings and testimony are also reflected in this study. While hearings can be problematic, due to the dynamics of testimony and the interests of witnesses, documents from those hearings are pertinent. In June 2009, a Congressional subcommittee held hearings on cyber security, current and emerging issues on identity theft in addition to, the improvement of private and public assistance to identity theft and current and emerging issues of identity theft. News correspondents who reported on identity theft were also monitored, as providing leads to recent cases.

(ii) Interviews

The second part of the research involved gaining more empirical data from interviews with key stakeholders in the criminal justice system involving identity theft and fraud. The interviews conducted, both informally and formally, for this project, were constructed based on a series of ongoing concerns by the investigator. These questions were not included in a formal survey, but utilized as a battery of questions to serve as a guide during the interviews. The overall methodological framework for the process of interviewing was ethnographic, that is, grounded in my experience in and familiarity with the milieu in which all of the interviewees were situated. Hammersley (1990) argued for studying people's behavior in everyday contexts, rather than under experimental conditions created by the researcher. To meet this criterion, field studies and surveys were assessed, in addition to perusal of the empirical data. Malinowski (1961) in defining his principles of methods stated:

Ethnographic sources are of unquestionable scientific value, in which we can clearly draw the line between, on the one hand, the results of direct observation and of native statements and interpretations, and on the other hand, the inferences of the author based on his common sense and psychological insight (1961:3).

This was the approach that was primarily adopted in this study. Fox and Lundman, however, (1974) have shown that:

Gaining research access may be conceived as a processual phenomenon involving a passage through two "gates." The first gate is manned by top-level administrators of the organization while the second gate is controlled by the aggregate group of proposed subjects of one's study. Access is successful when each "gatekeeper" approves the research (Fox and Lundman 1974:53).

The two gates which had to be negotiated within the criminal justice system in New York City were the commanding officer and detectives who are assigned to the Identity Theft Unit within the New York City Police Department and the Special Agent in Charge of the Electronic Crimes Task Force within the New York office at the United States Secret Service. Officers within the two gates were involved in all aspects of the Unit's field investigations, files, data analysis and undercover work. After a brief synopsis and explanation that this research project would reflect on only closed cases and that the investigator would be sworn to secrecy, some officers known from previous investigations co-operated with my questions in a controlled environment, resulting in significant results.

Additional obstacles experienced were not limited to the two main gates. This study was marked by early disillusionment due to encountering a "lock" on the gates within the identity theft unit at the Manhattan District Attorney's Office. Despite seventeen years of service, access to closed cases that are part of public record was not granted to me. This forced me to seek out other resources, using interviews, which potentially produced a more comprehensive and objective study.

The difficulty experienced in obtaining data from the department, also necessitated that the interviews with criminal justice professionals, victims and offenders be more comprehensive. In this theoretical context, interviews focused on a series of pre-established concerns. First, the study focused on the inadequacies of data collection and measurements, and the effective reforms that are needed to change the scope of identity theft. Second, the study addressed the economic and social impact of identity theft around the nation and specifically, in New York City. Third, the study addressed the motivation for criminal opportunity and the absence of proper guidance. If fraudulent individuals feel identity theft opportunities do not exist, they will not

commit these crimes. Fourth, to comprehend the State statutes on identity theft, I addressed several legislative issues regarding identity theft and fraud on the national as well as the state level.

Questions addressed to investigators or officials in police departments or other interested stakeholders were varied, focused on the dynamics of prosecution, the ease of prosecution, barriers to prosecution, overall department or industry response to identity theft and overall perception of the scope and scale of identity theft as a problem. The schedules used with each group of respondents are shown in appendices 3-5.

Based on the responses to these questions, follow-up questions would ask the respondent to expand on his/her original answer. This allowed me to focus the interview on the relevant details needed for this study.

(iii) Data collection, Processing and Analysis

The questions derived from the interviews with offenders, victims, colleagues and departmental officers were codified based on a desire to come to an answer in the following research questions, guiding the research:

1. What is identity theft?

2. How did identity theft evolve as technology and cyberspace became readily available to the general public?

3. Who are the identity thieves, what methods do they use in committing identity theft and how did they acquire the skills that are needed to commit identity theft?

4. Who are the victims of identity theft, how do they expose themselves to the identity theft and how has identity theft altered their activities and behavior?

5. What have been the strategies of the executive and the legislative branches of government (the criminal justice system), including law enforcement, to address identity theft and what challenges do they face in their effort to detect, investigate and combat identity theft?

My formal interview method entailed a broad coverage of all of the issues under discussion. In informal interviews, on the other hand, defined as interviews constrained by time or circumstance, and also based on questioner appraisal of the appropriateness of the question given the identity of the respondent—that is, investigator, offender or victim—a more limited battery of questions, possibly only covering one or two topics, were derived. While conducting most of my observations and interviews to acquire required data, I took hand written notes during or immediately following the interviews. These were then codified into themes according to which above research question they contributed to answering. From an analysis of convergent themes, conclusions were drawn.

(iv) Instruments

Some of the data analysis conducted for this study was comparative, that is, involving comparing the perceptions of respondents in interviews to questions about the nature and extent of identity theft, and then, in order to determine if their knowledge was limited or extensive, the degree to which their answers compared to the current level of knowledge about identity theft as indicated by a baseline measure of data discovered in the review of literature. A simple comparative benchmark was established for the level of knowledge of each group of respondents,

less than, about equal to or extending beyond the findings of the current research. It was hypothesized, given the researcher's experience, that the knowledge of most respondents will be limited and fall short of best practice.

Therefore, a new model for identity theft is required to improve their level of knowledge of the nature and extent of identity theft. For this purpose, routine activities theory was chosen as the primary lens through which the study examined the problem of identity theft. The instruments created to guide interviews of investigators, officials, offenders and victims, were tailored to each type of participant (see appendices 3 through 5). In the triangulated conceptualization of crime under routine activities theory, questions were included which focused on routine activities theory as it applies to both real-world and online scenarios of identity theft. Investigators and officials were interviewed as to their appraisal of factors in offender motivation, target suitability and guardian presence or absence and the incidence of identity theft. Their overall level of knowledge about the dynamics of identity crime was then compared to responses from other parties. Offenders were questioned regarding what motivates them to commit a crime, how they committed a crime and what made it possible for them to do, both on the street, in life or online. Victims were questioned about the extent to which their behavior created opportunity for crime both on the street and online, and if they have taken onto themselves guardian roles by changing their behavior to a more defensive stance. The population of offenders and victims were limited to those made available to the researcher through the course of research.

With regard to the motivated offender, RAT has found that victims are chosen based on: the least amount of effort, obviousness and most likely to produce results they seek. It is argued

that offenders undertake a rational choice decision-making process based on these decisions before committing a crime. With regard to target suitability, which increases the likelihood of victimization, crime is engendered by the least amount of challenge, participation of the target in careless activity, value, or the target's worth, inertia, or the physical weight or portability of the target, visibility, or if it is in plain sight or not, and access, or daily habits or routines which make a target easy to plan a crime against. Also, absence of guardianship measures lack of officers in the vicinity, lack of officer awareness of the potential for crime, lack of their superior's awareness of the locales or hot spots of crime, and presence of neighbours, friends, bystanders or shop or property owners. The presence of guardians or guardianship can be measured based on whether they include controllers, which would entail personnel or other persons, or so-called supercontrollers, which are laws and regulations. Finally, the convergence of all three factors in a single time and place is measured.

For this study, it was thought that a broad setting for identity theft, including the internet, was required, in order to provide a fuller picture of the problem of police enforcement than that provided by Fell (2009). Therefore, questions were adapted from Hutchings & Hayes' (2009) study on online user response to phishing emails. In this scenario, a motivated offender is defined as an offender who sees that phishing is easy, the suitable target is a user who responds to phishing emails, and the absence of a guardian would entail failure by the email server or website to provide any sort of protection against spam or phishing emails. Hutchings & Hayes (2009) were also interested in guardian response to current circumstances through the preventive responses of target hardening, in which suitable targets are hardened by increasing the risks and decreasing the rewards of committing a crime against them, and, online, this would include more

use of passwords and firewalls, and deflecting offenders, which involves reducing the opportunities for crime, in the case of phishing by the use of email filters. Hutchings & Hayes (2009) also focused on surveying victims and for that purpose developed an instrument which measured computer experience, internet experience, measuring purposes of Internet use, average number of hours on the Internet per week, number of email addresses held, and whether or the not user was trained in Internet use; access from home, work, university or school, friend or relative's home or another location (such as by WiFi at an Internet café) were also questioned; levels of Internet banking, including how often they checked their account balance, transferred funds, paid bills and how many bank accounts they accessed online, and if they had ever been employed at a bank; and phishing victimization, including use of filters, as well as demographics. A similar line of questions were derived with regard to other forms of online identity theft identified in the research.

The above questions, relevant to the research questions of the study, as well as a battery of questions derived from the above survey instruments, gave shape to the interview schedule which guided, but did not dictate, interaction with the interviewees.

The results of interviews from investigators, officials, stakeholders, offenders and victims were also, finally, compared against the previous in-depth research into departmental records on identity theft crime incidence as well as the battery of laws passed to combat identity theft, to come to a general comparative appraisal of the adequacy of law enforcement response to date.

It is was hypothesized that, due to the focus of law enforcement, investigators would have a greater knowledge of the nature and extent of identity theft at present, compared with officials,

but that both, due to elements of police culture, might still have conceptualizations of the nature and extent of identity theft that falls short of current reality. It was therefore hypothesized that the guardianship required to prevent identity theft is in absence or inadequate, with the law enforcement in particular challenged by the threats of online identity theft. It was also hypothesized that this shortfall of conceptualization, limiting preventive practice, is likely due to the dynamic between offender motivation and suitable target at the current time. That is, offender motivation remains high because of the absence of guardianship and the fact that victims continue to behave in under-educated ways both on the street and online with regard to protecting their identity that makes identity theft, compared to other crimes, easy, with little threat of consequence. It was also hypothesized that the responses from both offenders and victims will reveal various factors occasioning identity theft that go beyond the current extent of measures provided to explain crime even according to routine activities theory, with, for example, factors of target suitability, value, or the target's worth, inertia, or the physical weight or portability of the target, visibility, or if it is in plain sight or not, and access, or daily habits or routines which make a target easy to plan a crime against, at present, remaining highly vulnerable, and evolving quickly, opening up ever newer motivations for offenders to become involved.

(v) Confounding Factors

It is also true that data collection had to take into account the fact that a great deal of resistance was met during the investigation, likely stemming from either the difficulty obtaining trust from an active investigator in the field, or due to the so-called blue code or wall of silence which protects most police business from public scrutiny. This resistance was a primary cause

for formal interviews devolving into more informal self-structured interviews. With regard to officials, some assistant district attorneys at the Manhattan District Attorney's Office were forthcoming with information on the activities of identity thieves in settled cases. With regard to lawyers, despite explaining that the information requested for the investigation was public information, some attorneys were uncooperative. With regard to offenders, my professional experience provided me with access and the opportunity to research activities of identity thieves, including their methods and operational abilities. Additional detailed information was also gleaned while assisting with wire-taps, subpoenas, orders to produce, prisoner transport, interviews, the extradition of convicted felons and witness protection. To take this aspect of data collection into account during data analysis, data was coded based on source and weighted based on a scale of situational dynamics (formal-informal, full-partial, direct-indirect, impartial-partial, reliable-less reliable, expert-common knowledge) and these values taken into consideration in the final analysis of themes. The basic method utilized to ensure the validity of any data made use of in the data analysis was triangulation (see below).

An example is provided below of how in the course of professional activity related to my work as an investigator, contact with colleagues sometimes, by chance, occasioned formal interviews. My attendance at a conference on identity theft further revealed the difficulties of obtaining data on the extent, scope and degree of attention paid to identity theft in criminal investigation, but also the favourable happen-stance that sometimes brought data my way. On September 12th, 2010, the researcher was invited to join a panel discussion on identity theft which was held at Utica College in upstate, New York. My friend, retired officer, "XYZ" had been assigned to the Manhattan South, Grand Larceny Task Force, and accompanied me to Utica

College. He decided to stop by the unit to pick up memo book cards which displayed identity theft offender's personal information, photos, and a synopsis of their crime record, which were to be used as part of my discussion at the college. When XYZ turned to speak to a former colleague, I was confronted by plain-clothes detective A, who asked if I was "on the job" (police jargon for if I was a sworn officer), and if so, where was I "housed" (meaning where did I work). I showed Detective A my "tin" (shield) and explained I was on the job and assigned to the DA's Squad. This gave me insider status and enabled me to conduct a 90 minute interview with Detective A about his experience with the identity thieves. Afterwards, he filled out a questionnaire with mostly autobiographical information of some thieves. The Grand Larceny Task Force records consisted mainly of technical arrests data: description material and observations recorded for specific purposes by non-social scientists who work in the legal environment. I handed Detective A my business card and told him to reach out if he needed help from my office in any way. I thanked him for the information he provided and left for the panel discussion with my friend. Data obtained from this contact would be measured as indirect contact, previously unknown to me, but he submitted willingly, and cooperatively, to a full, formal interview and is an investigator, though not an expert in the field of identity theft. This episode demonstrates the opportunistic nature of some of the interviews conducted during the course of the research.

On the other hand, in order to frame the interview process by which data to be analysed for this study was extracted in the realities of the often-resistant context in which it was collected, one anecdotal scenario discussed below suffices to characterize the climate insofar as in this case communication with the respondent resulting in a refusal of a request for an interview.

Nonetheless, this experience generated valuable indirect or collateral communication that contributed to a research point in the study (the inadequacy of data). My initial experience in contacting a well-known crime reporter who is assigned to the press office at Police Headquarters was not met with enthusiasm. In my initial conversation with the reporter, my enrolment as a student at Cardiff University, Wales, U.K., was explained to the reporter via telephone, and permission was requested to speak to him and his colleagues at the press office about the identity theft articles that they cover. Surprisingly, the reporter put me on hold for a few minutes, returned to the phone and informed me that the research assignment that we discussed was impossible to carry out because no one was willing to spend the time conducting an interview on the topic of identity theft. Therefore, though my access to the reporter was not successful in terms of querying him as to his perceptions of the issues at hand regarding identity theft, the experience of contact with him, and his negative response, also provided me, through collateral communication (in which indirect remarks surrounding refusal to make direct statements elicit information) with pertinent data linked to both my professional role in the District Attorney's office but also to the culture of either silence or lack of concern over identity theft in criminal law enforcement. More specifically, while the initial interest in contacting a crime reporter was due to the fact that he would be knowledgeable in the field, and have sources within and outside of various organizations involved in criminal investigation and identity theft, the larger question was the extent to which a crime reporter would be willing to divulge his sources, how long it took for him to develop these sources and the extent to which reporter silence about sources contributed to silence about identity theft. By determining, even in rejection, that the reporter expended a considerable amount of time and effort to develop sources, was protective of his resources and would not divulge them, and would not talk to me because

most of his data was based on sources, the goal of establishing the complicated intersectionality of the flow of data about identity theft in crime investigation was confirmed. Data from this source would be coded as indirect, non-cooperative, involuntary, but expert.

Reliability and the accuracy of vital information are both crucial for the successful outcome of criminologist's research. Every effort, therefore, was made to ensure that; overall, the quality of data obtained in research was high. For the interviewer to be trusted, the interviewee must be comfortable and willing to engage in an interchange of views and ideas. A concerted effort was made to obtain as much information concerning identity theft as possible during the interview while asking the general questions that needed answering. Throughout the interviews a "big ears, little mouth" approach was adopted, an optimal method of interviewing learned over the years as a result of conducting criminal interrogations. Much can be learned and understood from listening. Miner (1984) shows that good listening like good interviewing requires patience, restraint and a degree of insight. Those that were interviewed were made to feel like they were the essential figure in the interview. By being an active listener, my subjects expressed themselves freely in long responses. The interviews varied from 90 minutes to three hours as there was no need to commit to a time frame. It is important for a qualitative researcher to conduct depth interviews but the difference between a depth interview and an interrogation must be clearly understood (in this study, a depth interview was classified as formal, one less so as informal) (Patton, 1987).

Some interviews were tape recorded with permission from the interviewees. However, many individuals were reluctant to be recorded. Some participants felt that a tape recorded interview was overly reminiscent of prior probing by police officials, which they resisted. When

practical, notes were taken during the interviews to capture major points discussed. Alternatively, notes were recorded immediately following the interviews while the thoughts and responses were clear in my mind. In addition, the taped interview notes were transposed immediately to allow for continuity of the note taking system that had been developed. Time spent around participants in court allowed insight into their daily routine as well.

In the case of Jake, who would sleep with two women per night, the hotel employee, who dumpster dove after hours, Michael, who undertook a rigorous daily routine of subway pick pocketing, and Bob, who engaged in meticulous and relentless casing of suburban homes, all engaged in enormous effort to get the information they needed, meaning that they were motivated by its current value more than anything else. Routine activities theory does state that the physical weight or portability of the target is a determining factor, and it is certainly true that most respondents appreciated theft only involving wallets, cards, and, even more portable, paperwork. The current research on identity theft, in accordance with most laws, seems to have fixated on formats of information, especially credit cards or debit cards. But Bob and Jake especially seemed aware that personal information of all sort was exploitable: thus, there seems to be a growing awareness that it is not about the format but about the information in the abstract. In this regard, the most eye-opening paradigm-changing observation was made by Bobby, burglar of suburban homes, who indirectly indicated that whereas formerly he might have paused to lift a television, electronics, jewellery, or other goods, to be later fenced, the focus of his gang today was to go right past these to personal information, of any kind, to the extent that they would take on the added tasks of lifting whole drawers of paperwork. Thus, a conventional crime is transformed by the focus on identity information into a new crime. The further de-

materialisation, as it might be called, of identity theft, was evinced by Joe's fixation of the mother's maiden name, and all of the false paperwork that it can generate. Where this awareness ends up is that all one needs is names, numbers, secret coded data, and not the physical elements: one can "steal" from a debit card that still resides safely in a consumer's wallet, no crime apparently committed, by allowing an associate to pay for an overseas hotel room with the stolen number. Also with regard to routine activities, it appeared that most respondents exploited people going through their daily lives, on subways, going to work, staying in hotels, and going out at night. In the case of Jake, who went home with women, and Bob, who posed as a delivery boy or gardening, criminal intent was disguised under routine business that would disqualify the oversight of either neighbours or police. It would appear that in all aspects of daily life, most people, by continuing to carry multiple pieces of ID in wallets, by not securing personal information in their homes, by tossing out credit cards slips in hotel dumpsters, by carrying PINs and Social Security Cards in wallets, continue to be generally unaware of the full dimension of identity theft. Finally, the overwhelming aspect of routine activities theory validated by my interview-based research was lack of preventive guardianship. One hundred per cent of respondents reported that they got into identity theft because there is little chance of being caught, or, if caught, much less punishment. This impunity was expressed on many levels, observing little detection on site (though Michael was apprehended on a subway), little chance that, if reported, police could conduct an investigation in a timely manner (though the hotel employee was eventually apprehended by a hotel guest who reported the theft), the grey areas of police jurisdiction in the overseas dimensions of the crime, the laxity of the judicial system, and the fact, as Joe mentioned, that even in prison, a paper-based crime like identity theft can continue to be conducted. As a result, it has to be concluded that at present, according to routine activities

theory, a perfect storm of high offender motivation, high suitability of target and low level of guardianship has made identity theft the crime of choice, and likely to be the crime that more criminals move into.

(d) Methodological Assumptions

The nature of my ethnographic approach, immersed in the experience and culture of the respondents, makes my methodological assumptions more pertinent. It was assumed that, in a culture generally reluctant, for various reasons, to discuss issues involved in ongoing investigations, completed investigations, crimes committed or crimes committed against them, all respondents answered my questions truthfully, honestly and in good faith, if only because, where the norm was silence, their willingness to participate indicated an interest in contributing to greater transparency and focus on identity theft. At the same time, it is assumed that methodological devices (noted above) to glean data from even involuntary or collateral communication would result in data that was nonetheless still pertinent.

(i) Limitations

Limitations of the study are apparent in the above-mentioned scenarios whereby data was obtained from investigators, officials, offenders or victims. That is, the circumstances of data collection resulted in informal interviews being the norm, though time was sometimes made for formal interviews, as indicated, meaning that the results from interviews were inconsistent in their coverage of all of the required research questions. This study examined numerous sources across several jurisdictions, agencies and individuals. There was potential for bias as subjects might be telling me what I wanted to hear or not giving valid answers. Participants who were not fully committed were not allowed to partake in the study. I also realized that my own

participation was vital in this important development. The participants were also limited to the above-mentioned departments and jurisdictions, and generalizing the conclusions of this study to other jurisdictions should be approached with caution.

(ii) Ethics

The ethics of an ethnographic study is complicated by issues of conflict of interest, and by the fact that as a working investigator in the field under study communication may be not forthcoming due to professional and other conflicts. In all cases, therefore, starting with receipt of permission from New York County District Attorney Robert Morgenthau, to every request of interview, my identity was made clear, my intentions were made clear, confidentiality, where appropriate, was assured, and all knowledge obtained was voluntary and neutral, that is, utilized solely for the purposes of the investigation.

Professional ethical issues particularly arose when it came to interviewing criminals convicted of identity fraud. Initially, concern was felt by myself and expressed by others regarding the ethical dilemma of an employee serving in one of the world's largest law enforcement agencies to be associated with known criminals. For a detective to be engaged with a confidential informant, official permission must be granted by the Chief of Detectives. However, acting as a researcher and not as a practitioner in my field of work meant that there was no obligation to seek official permission. This distinction, however, made it additionally important that at all times my role as researcher, not investigator, is emphasized.

The fraudulent individuals interviewed during the study were also cautious in the preliminary stages as they were unsure as to if, based on my different roles as investigator and researcher, my confidentiality could be trusted. It took some time for them to relax. No attempt

was made to hide my identity from the interview subjects, even if this identification resulted in rejection and distrust.

Some ethical dilemmas also arose in the choice of offender subjects. For example, to learn about identity theft, contact was re-established with a confidential informant with whom contact had been made several years earlier while working as a detective. My previous experience with the subject involved arresting him for robberies and later for committing welfare and white-collar fraud. My informant, identified by the alias "Charlie Hustle" had maintained a working relationship with me over the years, as an investigator. Returning to him as a researcher, and no longer an investigator, but, as a researcher, nonetheless exploiting a relationship formed while an investigator, at times seemed clouded by grey areas with regard to the importance of the above-mentioned ethical issue of clearly separating my previous role as investigator and current role as researcher.

Charlie was also instrumental, however, in introducing me to other fraudsters, some of whom were incarcerated for identity theft in the previous years when they were prosecuted under the Grand Larceny Statute, and others who are still "into the business" of committing other types of fraud, along with those who, in prior years, committed crimes such as bank robberies, burglaries, and assaults. This also meant that my investigation entailed contact with known and active felons. Since some of these individuals were not previously known to me as an investigator, access to them forced me to focus on my role as researcher, not to exploit this knowledge and access for investigatory purposes.

Contact with the offender population of respondents also required that the questions asked were adjusted so that interviewees would feel relaxed and comfortable. Even though most were educated beyond the high school level, an effort was made to speak to them using street

terms. By doing so, it was found that this direct mode of interviewing resulted in better communication and trust. Whether or not this trust, however, was authentic, or placed the agreed upon researcher-respondent relationship in jeopardy, in various ways, was still another ethical dimension unique to this research. But it is also true that this trust enabled me to ask additional questions after receiving the first answers so that complex questions or answers can be simplified through further discussion. Because of the uncertainty of an offender consenting to follow-up interviews, as fraudsters and other criminals can be difficult to locate, a concerted effort was made, with this population of respondents, to conduct my interviews in single, long one-on-one sessions to avoid repeat or supplemental interviews.

Interviews with offenders also raised additional ethical questions. Harold, a police informant, was highly recommended to be an interview participant and was recommended by another informant with whom I had worked in my official capacity. Harold was interested in the topic of my research because he served time in state prison as an identity theft felon and was on parole. Before we sat down for the interview, however, Harold was, with reluctance on my part, given one hundred and thirty five dollars by me to pay his phone bill, as he lamented that his phone was due to be disconnected. As a result of this payment, the interview was given and Harold also made himself available for follow-up interviews. There is nothing unusual about an exchange of money for an interview in police culture. Informants will generally exchange information concerning these activities provided they are compensated for such information. Criminals always feel that they should be compensated, and are often unwilling to cooperate if they are expected to give up any thing they possess “for free”. People always have an ulterior motive whenever they give up this kind of information, and it is not uncommon for informants to be compensated by personnel from law enforcement agencies in exchange for information. Far

from being viewed as a form of corruption (in effect, a 'bribe,' but directed back at an informant), exchange of minimal amounts of money is viewed as a symbolic gesture of trust, expediting communication. Given this reality of the criminal culture, my assumption is that payment did not compromise the veracity of interviews, that is, the money exchanged was not sufficient to motivate offenders to tell tales in order to "earn" more money from the process, especially as any payment was minimal and made with an understanding that it was one-time-only.

(iii) Validity of the Study

Social scientists have emphasized confidence in the importance of triangulation in the results of empirical studies (Campbell 1966; Denzin1978; Denzin and Lincoln 1994). Results from interviews, observations, recordings and researched court data were utilized to cross-validate the method used for the findings. For the method to be effective, the collected data must be of good quality. The validity of almost all of my collected data has been tested, through the triangulation (Denzin, 1970) of interviews, observations, recordings and published literary sources, such a multi-method inquiry reflects on Van Maanen et al. (1982) reference to the "triad." The triad presented me with a different vantage point to study the pertinent issues.

Therefore, methods triangulation was the best means for measuring my findings on identity theft. In addition, the research was prepared for the responsibility and consideration of my informants. However, the researcher must do everything within their power to protect their physical, social and psychological welfare and to honour their dignity and privacy (*Principles of Professional Responsibility,* 1971, para. 1). The judgement call incorporates my professional position, using sources developed during my seventeen years as a detective investigator. These opportunities afforded me access to field studies, journalistic accounts, and finally the analysis of the collected data, coupled with snowball sampling, has enabled me to validate my findings.

(e) Conclusion

This research consisted of an ethnographic study of the problem of identity theft, focusing on its pervasiveness today as well as the capacity of current policing practice to confront this new form of crime. The study took on an ethnographic quality utilizing research conducted in and around police departments due to the researcher's seventeen years of experience fighting identity theft and fraud from the investigatory team of the Office of the Manhattan District Attorney in New York City. The methodology of the project focused on collecting data from police departments as well as interviewing fellow investigators, senior officers, identity theft offenders and identity theft victims. Interviews were deemed necessary due to encountering lack of access and departmental silence regarding identity theft prevention and prosecution efforts. Hundreds of investigators specializing in identity theft, police officials and criminal justice prosecutors at various levels, industry stakeholders, 25 convicted identity theft fraudsters and 25 victims of identity theft were interviewed. From both informal and formal interviews, results were codified to gain insight into the adequacy of identity theft fraud data collection, the social and economic impact of fraud, the motivation of criminals committing identity theft and the current statutes against identity theft, in terms of their efficacy. Results were further analysed to answer the research questions underlying the project, including what is identity theft, how identity theft evolves, who identity fraudsters are and how they obtained the skills to commit their crimes and what strategies have been implemented to combat identity theft. Because this was an ethnographic study, ethics involving secrecy, confidentiality, and how to interact with convicted felons were given extra emphasis. In addition to the aforementioned interviews and due to the unavailability of statistical data of substance, 30 identity theft cases were studied for place and means of compromise.

(i) Routine Activities Theory

With regard to routine activities theory, the reports by respondents more or less confirm the model. Therefore, there were a few elements of routine activities not borne out. Routine activities theory argues that offender motivation is partly fueled by the least amount of effort in committing a crime...

Most of the interviews undertaken were carried out in downtime or collateral moments linked to law enforcement action. Almost all were relatively full, formal interviews, routinely lasting more than 45 minutes. In Jake's case, he prohibited me from taking notes, and finally left the interview prematurely, perhaps curtailing providing me with broader information on the scope of his activities. In Harold's case, a bill was paid as a way to get him to talk, but this did not seem to compromise the impartiality of his information. While conditions of Bobby's interview, originally reluctant, and at a time in transit when he was in shackles, might have constrained him, provision of privacy mitigated that. Therefore, coding these factors, my general conclusion is that the majority of the responses were valid and honest reports of actual identity theft behavior by these individuals.

(ii) Beyond the Individual

Finally, another dimension entered into the picture briefly, in my individual interviews, which then lead me to a broader study of the full scope of identity theft, that is, the involvement of organized crime. In the case of Joe and Bob, their involvement in gangs or organized crime, meant that they had much more sophisticated view of identity theft as it morphed and expanded into identity fraud. Identity theft could be defined as efforts undertaken to steal the personal data,

while identity fraud can be defined as all efforts undertaken by associates and others to exploit the stolen information, involving forgery, obtaining false documents, filing for fraudulent funds, welfare checks, food stamps, illegally purchasing merchandise, selling that stolen merchandise to other merchants, or overseas: fraud is the dimension where “identity theft” as a crime appears to be in danger of exploding to “intermestic” dimensions far beyond the capacity of location-based law enforcement agencies to manage or combat. As a result of this conclusion, some additional research was conducted into the scope of organized-crime run identity fraud rings, and the findings confirmed that identity theft has metastasized through several cycles of crime, and even become involved in other kinds of gang crime, to become a significant stream of organized criminal behavior.

The position adopted in this research is the virtue rational choice approach to the problems of identity theft violence; therefore, it gives a methodological conceptual framework on the basis of which some understanding of the crime can be developed and offers avenues along which initiatives to effect change can be empirically explored.

Chapter 4: Statistics, Trends and Patterns

Introduction

This Chapter presents the findings for the fourth research question posed for this study: who are the victims of identity theft, and how have they exposed themselves to identity theft in their activities, and what has been the impact of identity theft on their lives? The findings identify a number of activities and attitudes in identity theft victims that may contribute to the growth of this kind of crime. The findings, insofar as they developed data on routine activities by victims, also weigh in on the applicability of routine activities theory as a framework for police investigation and law enforcement prevention and as an adequate response to identity theft and fraud.

(i) Current state of Awareness

The Identity Theft and Assumption Deterrence Act of 1998 mandated the FTC to create The Identity Theft Data Clearinghouse. In November, 1999, the Clearinghouse was officially created to receive and collect data on consumer's (victims) complaints. Newman and McNally (2005, p. iv) (quoted in Pascoe et al. 2006), stated that "While there are some differences in the amount of identity theft by states, regions and to some extent age, the data shows that, depending on the type of identity that is being perpetrated, all persons, regardless of social or economic background, may become victims of identity theft". FTC (2011) figures indicated that an estimated 8.6 million households with persons over the age of 12 had encountered some form of identity theft by year 2010. These figures compared to 6.4 million victimised households in 2005, which was an increase of 2.2 million victims for the five year period. The increase in household identity theft was the result of the fraudulent use of credit cards along with other

accounts, namely utility and banking accounts. Thus, the misuse of credit card accounts increased from 3.6 million in 2005 to 5.5 million in 2010. Approximately 35% of victimised households experienced the fraudulent use of other business accounts, which remained unchanged from year 2005 through 2010. Households headed by non-Hispanic Whites, Asians and Hispanics reported an increase in identity theft from 2005 to 2010. Households headed by non-Hispanic Blacks, African Americans, Native Americans and persons of two or more races did not experience a change in identity theft. A financial loss of approximately $13.3 billion was experienced by U.S. households. Additional financial losses were the result of thieves misusing personal information to create new accounts. Each household suffered an average loss of $13,200. Additionally, the misuse of active credit cards was responsible for an approximate 30% financial loss with a combined loss of 54% victimisation.

(ii) Measurement of Identity Theft

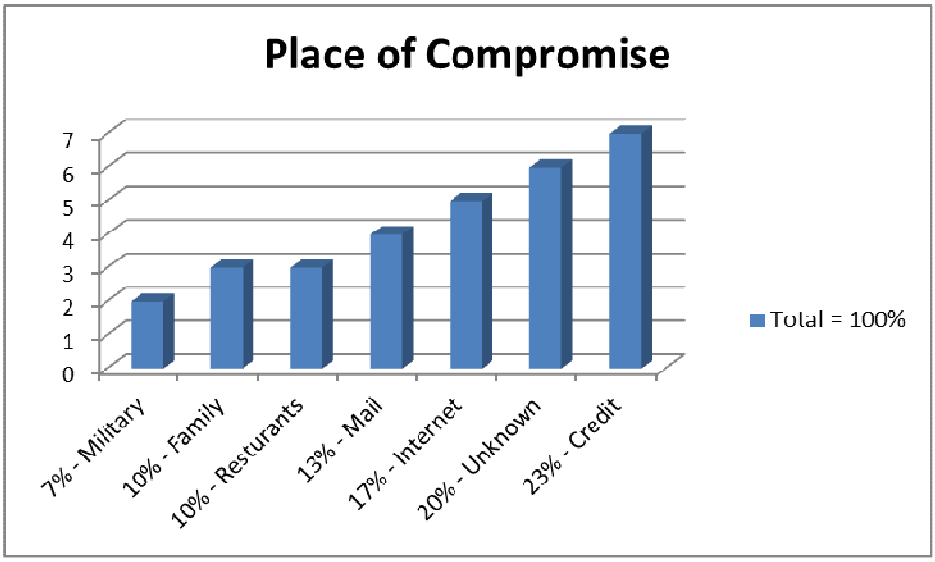
Hayward (2004) in her overview of identity theft concluded that there are no comprehensive statistics on the prevalence of identity theft. It was therefore a difficult task to support interviews with data that were completed with law enforcement officials from such agencies such as, the Department of Justice, the US Attorney's Office, the Postal Inspection Service and the FTC. From those interviews it was apparent that there is no single database in the United States that shows a true picture of all identity theft fraudsters or victims. This is likely because some victims choose not to report the crime in the first instance, and others may not be aware they are even victimized until months after their identity is stolen. Some victims also do not report the crime because they feel that nothing can be done because of the passage of time.

A canvass amongst several officials assigned to the above agencies revealed that it is extremely difficult to measure the amount or even trends of identity theft fraudsters or victims

because federal law enforcement agencies do not have information systems that facilitate specific tracking of identity theft cases or complaints. Identity theft is almost always a component of white-collar or financial crimes such as bank fraud, credit card fraud or the use of counterfeit financial instruments. The Consumer Sentinel Network (CSN) collects complaints filed with the Better Business Bureau, the Internet Crime Complaint Centre, the National Fraud Information Centre, The U.S. Postal Service and others (CSN, 2010:2).

In response to the lack of organized statistical data on identity theft, an original study was conducted by this researcher who analysed 30 identity theft cases in order to distinguish the actual means and locations of occurrence of identity theft crimes. The information is reflected in the below listed (place of compromise) chart. After examining 30 identity theft cases, results shows credit card fraud as the most common form of compromise and military the least. Upon further examination of the cases, it was realised that a table was appropriate. Table 3, as shown below, shows places of compromise range from military (7%), followed by family and restaurants (10%), mail (13%) internet (17%), unknown (20%) and credit card (23%).

Table 3
Number of Identity Theft Cases (30) Analysed for Place of Compromise



Note: Seven categories in the above table (table 3) were examined for places/source of compromised. Military showed the least form of compromise while credit card was the highest (noted in appendix 1.).

(b) Consumer Reporting Agency Data

The collected statistical data information in the first instance is as reliable as the individuals reporting it. The data is based on voluntary reports by individuals who purport to be victims. Reports are received by civilian agencies, as well as, law enforcement and are presumed to be reliable. On the other hand, victims are not mandated to report these crimes. After the reporting entities send the information to the repository such as the FTC, the data is collected and used for statistical reasons. The FTC is recognised as a reliable repository agency as their web site is more readily accessible than other comparative sites.

(i) Official Data

When the Federal Trade Commission (FTC) began compiling identity theft complaints in November 1999, the agency initially received an average of 445 calls per week. By the

beginning of 2002, the average was 3000 calls per week. By 2009, there were several conflicting numbers for the amount of calls received by the FTC and other clearing houses. However, the FTC's main focus is on consumer awareness and not fraud detection. The Consumer Sentinel Network (CSN) Data Book contains over 6.1 million complaints dating from calendar year 2006 through calendar year 2010. The CSN received over 1.3 million complaints during calendar year 2010: 54% were fraud complaints; 19% identity theft complaints; and 27% were other types of complaints. Identity theft was the number one complaint category in the CSN for calendar year 2010 with 19% of the overall complaints, followed by Debt Collection (11%); Internet Services (5%); Prizes, Sweepstakes and Lotteries (5%); Shop-at-Home and Catalogue Sales (4%); Impostor Scams (4%); Internet Auction (4%); Foreign Money Offers and Counterfeit Check Scams (3%); Telephone and Mobile Services (3%); and Credit Cards (2%). The complete ranking of all thirty complaint categories is listed in the CSN report. Government documents/benefits fraud (19%) was the most common form of reported identity theft, followed by credit card fraud (15%), phone or utilities fraud (14%), and employment fraud (11%). Other significant categories of identity theft reported by victims were bank fraud (10%) and loan fraud (4%). Government documents/benefits fraud increased 4 percentage points since calendar year 2008; identity theft-related credit card fraud, on the other hand, declined 5 percentage points since calendar year 2008. However, between January 2000 and 2009, identity theft was the top complaint category and credit card fraud was the most common form of reported identity theft (FTC 2009, 2010).

A Javelin Strategy, Fraud and Survey Report (2010) showed 11.1 million adults in the U.S. were victims of identity theft in 2009, compared with 9.9 million victims in calendar year 2008. These figures reflect an increase of 12.5 percent in the amount of $54billion. Identity theft,

although a significant, serious problem appears to be levelling out as indicated by the. Additionally, studies show that identity theft is done by exploitation of existing accounts. The FTC's, Consumer Sentinel report (2012) shows that for calendar year 2011, consumers filed more than 1.8 million consumer complaints which included over 279,000 for identity theft. These figures are left to interpretation because there is no single repository for consumer identity theft complaints.

The following two main sources corroborate these trends:

(ii) Official Reports

In 2004, the Financial Crimes Enforcement Network (FinCEN) began to focus their attention on identity theft in the securities and futures industries. This change occurred as a result of Suspicious Activity Reports (SAR) that was examined by the Securities and Futures Industries. At that time, the State and local governments had not begun to act on SAR's and was unaware of the new patterns and trends used by identity thieves to access and abuse trust accounts, as well as, investment and retirement accounts. At the time, it appeared that FinCEN was the pioneer in identifying the various methods used by the identity thieves to defraud securities firms and individual account holders.

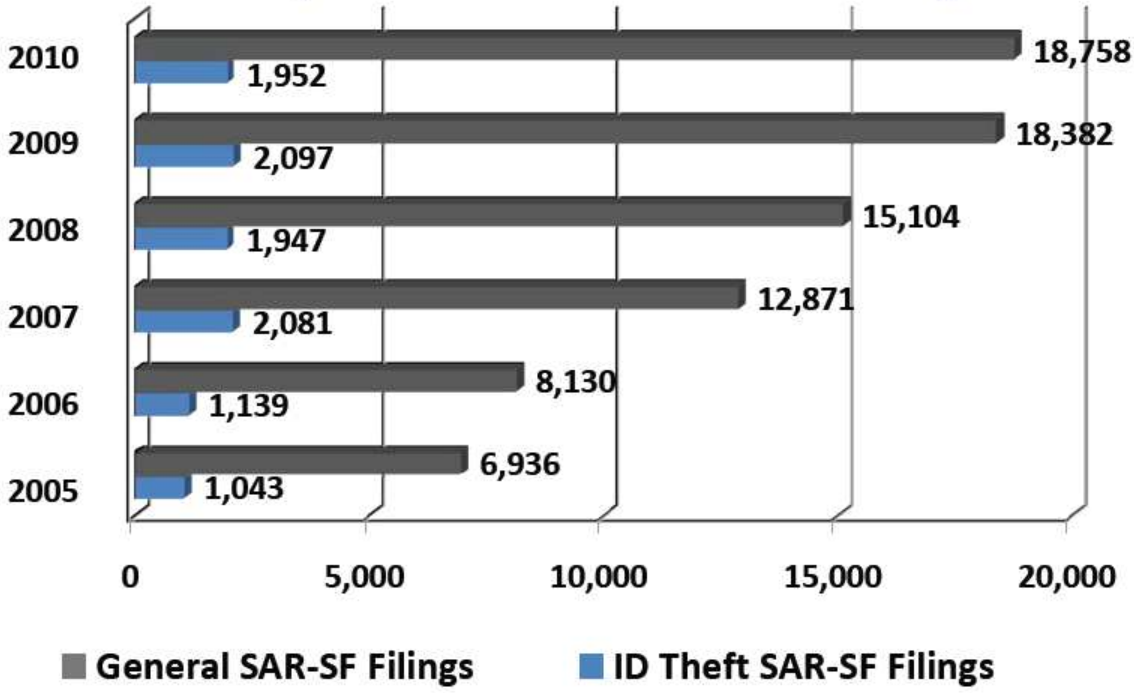
As stated, FinCEN pioneered a reported system which spurred the inception of the SAR review. Table 4 (which is cited below as Graph #1) is a review of US Department of Treasury, FinCEN, *Identity theft patterns and typologies Based on Suspicious Activity Reports*, filed by the Securities Futures Industries from calendar year 2005 through 2010. For the purpose of this research, figures for calendar year 2009 and 2010 that are shown in table 4 (below) will be

compared with actual statistics which were compiled by personnel in the New York County District Attorney's Office for calendar year 2009 and 2010 and will be further illustrated in table 5. This researcher is presenting these figures to show the steady increase in the intensity of identity theft. This illustrates the need for the various law enforcement agencies in the US, on the federal, state and local level to share their resources to eventually curb and reduce the trend in identity theft. The comparative chart will also reflect the number of cases generated by analysts in the District Attorney's office for investigative purposes. The graph in table (5)further illustrates that offenders utilize a network to accomplish their task. Identity theft is not only a lone wolf operation. It takes a planned coordinated effort which will be discussed further in this research.

Table 4

GRAPH 1

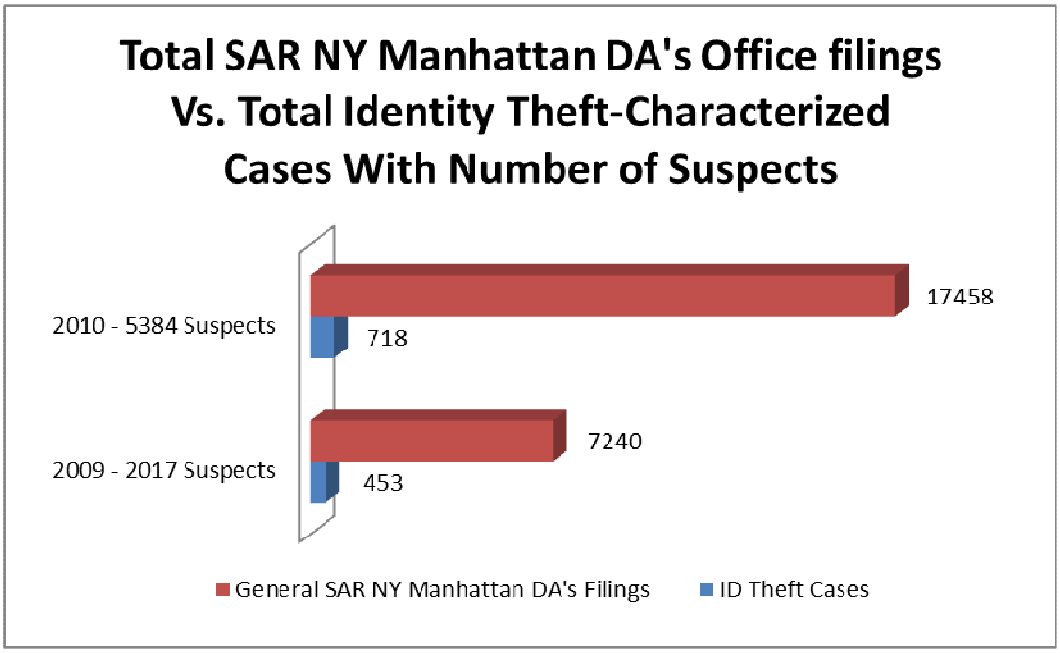
Total SAR-SF Filings vs.
Total Identity Theft-Characterized SAR-SF Filings



Source: Financial Crimes Enforcement Network *Identity Theft Trends, Patterns, and Typologies Based on Suspicious Activity Report*s Filed by the Securities and Futures Industries January 1, 2005 – December 31, 2010, p.1.

*Note: Table 4 (graph 1, for the purpose of proper citation only) shows the general number of SAR filings for calendar year 2009 (18,382), a when compared to 2010 (18,758). Table 4 also shows the number of SAR identity theft filings for calendar year 2009 (2,097) and 1,952 for 2010.

Table 5

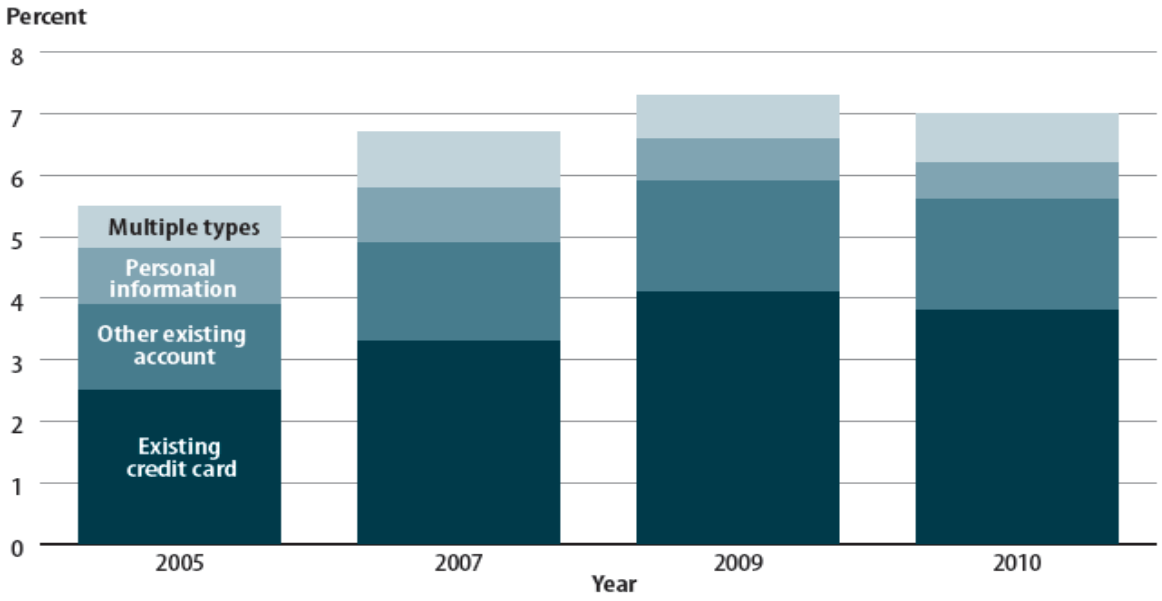


*Note: Table 5 shows the number of SAR reports analysed by personnel in the Manhattan DA's Office for calendar year 2009 (7,240) in comparison to calendar year 2010 (17,458). Table 5 also shows the number of identity theft cases for calendar year 2009 (453) compared to calendar year 2010 (718). The number of suspects generated from cases in calendar year 2009 and 2010 were 2,017 and 5,384.

The chart below Table 6 (figure 1) shows an increase in identity theft victimisation from 2005 through 2010. Existing credit cards was recognised as the cause for an increase in the misuse of existing credit card accounts. The data shows the percentage in households that experienced the misuse of an existing credit card account increased by about 50%, from 2.5% to 3.8%. The percentage of households that experienced the misuse of personal information to open a new account or for another fraudulent purpose declined by about 30%, from 0.9% in 2005 to 0.6% in 2010.

Table 6

FIGURE 1
Percent of households that experienced identity theft, by type of identity theft, 2005, 2007, 2009, and 2010



Note: There are no available annual estimates for year 2008 because only six months of data was collected.

Source: U.S. Department of Justice Programs Bureau of Justice Statistics Crime Data Brief November 2011 "Identity Theft Reported by Households, 2005-2010" By Lynn Langton, BJS Statistician. http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh0510.pdf - 2011- November.

(iii) Review of Research on Victim Response

Several of the findings of general research about identity theft apply to the situation of its victims, including the fact that identity thieves remain a moving target, difficult to identify (Wagner, 2009), more and more crime occurs on the Internet, in the form of phishing and malware, offenders view identity theft as a victimless crime (Copes & Vieraitis, 2007), and an increasing number of offenders are using stolen credit cards to obtain all manner of additional personal data with which they then take out new loans, incur debts, open other accounts and commit other crimes. General research as to the mechanisms used by offenders to commit identity theft indicates that credit card theft, debit card theft, bank account emptying and use of personal information to obtain loans remain the most common offenses (Bronk, 2008). The research also indicates that while offline theft remains more common, Internet –based identity theft is growing in prevalence (Berg, 2006). All of these findings are reflected in victim responses.

In terms of direct research into victim experience of identity theft, the research at present indicates that 61% of victims still fail to notify the police of a theft (Wagner, 2009), younger credit card holders are the most common victims (Fell, 2006), and most victims do not discover the theft until sometime after the stolen data has begun to be used to exploit their bank accounts, credit card accounts, and other property. As part of this research, victims were asked how quickly they became aware of the theft, what was the total dollar amount, how much time it took to clear up the problem, if theft resulted in any other negative outcomes and if they were forced to close an account, all to establish a level of awareness of these issues. Finally, victims also have views about how law enforcement responded to their reporting of identity theft. At present, if current law was effective, it would follow that victims would be most likely to hear about an identity theft through a red flag raised on their account either at work or by a security company

hired to monitor their bank account by the bank (Bose & Leung, 2009), or by a notification from a company against whom a debt was incurred based on breach notification laws (Burdon, 2011). In addition, one of the hypotheses of this study is that current police response to identity is hamstrung and ineffective due to jurisdictional and other issues, and that, as a result, routine activities theory is required to give structure to police response, to improve its response (Tillyer & Kennedy, 2008). Though it is likely that most victims will be in the dark as to who or how their data was stolen, it is much more likely that they will have come in contact with police officers as a result of the theft, possibly in inopportune ways, based on the extent to which the misuse of the stolen data put their name on some list that required police response. In the research, routine activities theory argued that for a crime to be committed, a motivated offender, a suitable victim and absence of guardianship must all come together in one place, to create an opportunity for commission of the crime (Mench & Wilkie, 2011). If police operated according to best practice in utilizing routine activities theory as a framework to focus their response to identity theft efforts would be made to reduce offender motivation, make the victims less suitable (by educating them not to engage in data-insecure behavior) and by providing more guardianship, in many different ways. The research has found that educating consumers could reduce Internet-based fraud.

(c) Data on Individual Cases

Twenty-five victims were interviewed based on the research questions and follow-up questions. A few victims are named anonymously; other victim identities were only numbered, and remain so in these short synopses of their commentaries.

#1 Linda

One afternoon in March 2005, I received a call from Michael. At the time, Michael was a police officer, who was assigned to the Manhattan South Grand Larceny Task force. Michael responded to the Saks Fifth Avenue Store uptown in Manhattan because security was "holding one" (police jargon for a person under arrest) for suspicion of identity theft. Michael asked if he and his partner could come up to the Squad room at the District Attorney's Office and process the "collar" (arrest) because they preferred to complete the arrest processing, which included an attempt at debriefing the prisoner, speaking to the prosecutor and lodging the prisoner in the Central Booking complex at the Manhattan District Attorney's Office. Permission was granted and about an hour later, the two officers arrived with the prisoner to complete the arrest processing.

The prisoner was a female and for safety reasons she needed to undergo a search for contraband and weapons; I was instructed to conduct the search in private. Towards the end of the search I discovered a secret pocket sewn on the inside of her jacket. The prisoner's jacket was removed to allow for a more invasive search. The secret pocket held thirteen credit cards. There were six American Express credit cards, five Master Card credit cards and two Visa credit cards. All of the cards bore the identical first and last name. Michael asked for help with processing the "collar" because his partner was meeting with the lead prosecutor on this investigation. I told Michael that I would give him a hand with whatever he needed. My Sergeant also gave me permission to help the two officers move the arrest processing along. After the defendant was read her rights, she agreed to provide Michael with a written statement. While the statement was being written, Michael asked that I call Linda, the victim, and interview her on the telephone because he needed a statement in order to move the arrest processing along in a timely manner.

While dialling the victim's telephone number, I realised that the 305 area code was assigned to the State of Florida. Michael informed me that the defendant and others had been at Saks Fifth Ave, shopping with multiple credit cards. At approximately 6:00 pm., I rang the telephone number. A young girl answered the phone and yelled, "Mommy!" A woman quickly picked up the phone and answered, "Hello." I introduced myself as Detective Newton, from the Manhattan DA's Squad. I informed the victim of the possible theft or compromised credit cards that were issued in her name. I further explained that someone was caught using the stolen cards at a retail store in New York City and that person was currently being held in police custody.

"My credit file was compromised about a year ago. My life had been pure hell. The debt collectors kept calling my house all hours of the day and even up until about 9 pm. at night. I spent time and money calling the credit card companies, but everything that I said fell on deaf ears because no one believed what I was saying to them was in fact true and that I am a victim of ID fraud. One day I received a call from someone at a savings and loan company asking for a deposit for my account that carried an overdraft. Fraudulent checks were presented against a checking account bearing my name; I saw many withdrawals that appeared on financial statements bearing my name and to add insult to injury. I remember one stormy night I received a call from an officer at the Florida Department of Law Enforcement advising me to come into his office in order to straighten out a confidential matter. It was at that moment when it hit me ... I better seek legal help."(Linda)

Linda felt a sigh of relief after venting about her identity theft problems. She thanked me for listening and also offered thanks to the officers who apprehended the defendant while expressing her willingness to testify if necessary. The interview lasted for approximately one hour and forty five minutes.

Analysis of Linda #1

In terms of the research questions, and sub-questions on the survey, Linda would be identified as an average consumer making use of banking in her everyday commercial life. It appears from bank response that she was informed of the problem fairly soon after fraudulent checks were presented in her account, though the fact that many withdrawals had been made suggests at least a few days or a week passing from incident recognising a problem. The fact that a savings and loan company called her indicates that in her case red flag rules flagged suspicious activity, and responded. As to her experience, the fact that her life was described as "pure hell" for over a year is reflective of other stakeholder response to her problem. Credit card companies had debt collectors calling her house in a highly aggressive manner, upsetting her daily life. A great deal of effort was expended trying to clear up the matter with these companies, but Linda felt that no one was listening, as they all acted under the assumption that she was overusing her cards and not a victim of ID theft. If several withdrawals had been through checks in her account and activity was reported on her credit cards one can assume that the total dollar amount was in the thousands of dollars. With regard to how much time taken to clear up the problem, a year later she was still in her "pure hell." Linda made no indication if she had closed her accounts or altered her behaviour as a result of the incident, nor was there any comment on what she might have done to make herself vulnerable to the theft. With regard to police response, she considered being called down to a police station to discuss the matter an insult, presumably because she was being assumed to be guilty of some malfeasance with credit card debt, and in fact sought legal advice, a clear sign of evidence of a sense of re-victimisation by the system. That said, insofar as the interview was conducted by a representative of the police, and reported that the criminal who had her stolen card in her possession had been apprehended provided her

with a sigh of relief (though why that card would not have been cancelled some time earlier remains an issue). The fact that the identity theft in possession of the physical stolen credit was operating in New York City, while the victim lived in Florida, undoubtedly exacerbated the problem in terms of local police response.

Barbara's sons #2

In July 2010, through an associate, I was given permission to interview Barbara, a single parent of 10-year-old identical, twin boys. Barbara informed me that her twins were victims of identity theft; the boys had been identified as two of the youngest victims of identity theft that arose from an official investigation in New York City. The interview was conducted at a restaurant named City Hall, located in lower Manhattan. Barbara informed me that she was formerly employed as a Senior Vice President at a financial firm, located in the World Trade Center up until its destruction on September 11, 2001.

Barbara: "I had scheduled Paediatrician visit with my boys on that fateful day. As a result, I was at home on the Upper East Side when the buildings collapse. I kept some valuables which included the children's birth certificates, social security cards and my husband's personal papers in a locked box, which was placed on a shelf in one of the closets in my office ... So I assumed that the locked box containing all papers was demolished from the impact of the explosion. About a year later, I learned that fraudulent credit cards, as well as, fraudulent accounts of several types were established in the children's names. My children's social security numbers were also used for employment purposes while withholding income tax. My twins were responsible for credit card accounts, personal and auto loans, checking and savings accounts as

well as utility accounts... We even received a bill for surgery in the amount of $70,000 from a Hospital in West Palm Beach, Florida. The thieves did not stop there. We are now receiving notice of delinquent loans from two credit unions along with inquiries on questionable purchases on credit applications." *Barbara, there are several ways to get help with your issues.* It was at that point in the interview when Barbara became very angry and with a look of despair on her face, she informed me that it was time to end the interview. I thanked her whole heartedly, picked up the $200 tab at the restaurant and offered to give her a ride home. She politely explained that her driver was waiting at the door.

Analysis of Barbara #2

Barbara was a Senior Vice President of a financial firm located in the World Trade Center, indicating that identity theft strikes highly-aware professionals in the field as well. Her personal data was not stolen, but data regarding her twin sons, contained in personal paperwork, were, and used for a wide range of subsequent fraudulent activity. The stolen data was accessed, in unclear ways, when a lock box with personal information and family papers in her office was compromised. The manner in which they were compromised represents circumstances that, when faced with describing it, words fail: that is, somehow the lock box was stolen or retrieved as a collateral event linked to the collapse of the World Trade Center. Barbara naturally assumed that the lock box and all data in it had been destroyed by the impact of the explosion, meaning she would not have thought of bringing the box with her when fleeing the scene. Again, it appears that she first learned of fraud through a credit card company working under a red flag rule, calling her to alert her to the fact that apparently fraudulent cards and accounts had been presented and established. The credit card company did not call to collect, but to inform,

according to red flag norms. However, the stolen ID of her ten-year old twins was used extensively to create additional credit card accounts, take our personal and auto loans, and open checking and also utility accounts. The stolen ID was also used to finance a surgical procedure at a hospital and the social security numbers were used for a fraudster to gain employment for the purposes of withholding income tax. The bill for the fraudulent surgery was $70,000, indicating that large amounts were involved in this fraud, presumably in the plus $200,000 range, or more. This also suggests that the problem persisted for some time, with Barbara indicating that she only was alerted to the problem almost a year after the theft. The fact that in this time other credit card companies began to notify her, not of theft, but of delinquent loans, also indicated that they had begun to accept the loans on face value. This interview is classified as partial, thus failing to gain information on how Barbara responded to the problem (though with her financial background one must assume that immediate action was taken, upon notification, in terms of closing accounts and clearing up problems), because Barbara's anger and emotionality over the theft forced her to end the interview prematurely. It is likely that the circumstances of this theft, that it involved not herself but her children, and that it occurred as a "collateral event" linked to 9/11, and the fact that her office, and, perhaps, almost her life, were destroyed in that event, being extraordinary, continued to make her response to the theft more emotional. No mention was made of police response; she was dismissive of the pat assumption-of-guilt response of debt collectors, whose practice seems based on assumptions based in a world without identity theft, and no internal mechanisms to be able to differentiate routine and suspicious behaviour.

Victim #3

My niece and I spent 13 months trying to clear my name from the identity thieves. They ran up credit card bills and even bought a car in our names. We were responsible for over $75,000 in debt. The police notified us and explained that the thieves were members of a gang that preyed upon elderly people. We were always very careful with our documents and we could not understand how they got hold of our information. We suspect my niece's 15 year old son who is a member of one of the gangs gave them access to our information. We were never more violated and when we called the police they were not sympathetic to us and acted like this crime is out of control. We were being held accountable for the bad credit that was attached to our names until my congressman intervened. We were forced to close our existing accounts and were issued new cards under new accounts.

Analysis of #3

3 was an elderly woman, and her niece, though it was unclear if the niece was also a victim. Notification in this case occurred; it would appear, through the police, who informed them that a gang had been using identity theft to prey on elderly people. The total dollar amount was high as the fraudsters ran up credit card bills and bought cars with them. The total provided by the interviewee was over $75,000 in debt. The woman reported that it took up to 13 months for her and her niece their clear their names and restores their credit. In this process, they were forced to close their existing accounts and were issued new cards under new accounts. With regard to how they might have acted to expose themselves to theft, they made a point of indicating that they were personally careful with personal data and could not at first understand how the data was stolen. It was then expressed that the niece's 15-year-old son, a gang member, passed the personal data to the gang (no substantiation of this claim was forthcoming). Police

and credit card company response in her case were both in a manner that could be characterised as re-victimising insofar as the police were not sympathetic, made them feel still more violated, and only expressed the notion that identity theft crime is out of control and there was nothing they could do. The fact that both the police and credit card companies apparently held the victims of identity theft accountable for the debts attached to their name deepened this sense of re-victimisation. In this case, the woman only was able to push back against two unresponsive stakeholders by having a third, her congressman, intervene. The interview with #3 is characterized as full as it touched on most of the major points being researched.

Victim #4

I have been the subject in a criminal investigation because my identity was compromised through a data broker. Thieves from outside of the US hacked into the broker's data bank and stole thousands of personal information. My file was included. Shortly thereafter, I received a notice from a credit reporting agency that numerous individuals attempted to take over my credit file. They also made credit cards in my name and attempted to use them at a large department store in New York City. I also received a call from Master Card inquiring if I was travelling in Moldova. I informed American Express that not only was I not travelling there but was unaware of where Moldova was.

Analysis of #4

#4 described the time from when the identity theft occurred and when he was notified as "shortly after". Notice was received by a credit card reporting agency of attempts to take over

his credit card account, indicating again that red flag and breach notification rules were responsible for first notification, in a fairly timely manner. The credit card companies were apparently highly suspicious of this case as clearly being identity theft because the totals and sites of credit card use were not typical of #4, a large amount in a New York City department store, and from a traveller in Moldova, with #4 being able to prove quite easily that he was not in Moldova at the time, and did not even know where Moldova was. Master Card seemed to accept this, as no sense of revictimisation is reported in #4's response. The amounts were clearly large, but not exorbitant. It appears that credit card company response prevented the credit card accounts from being fully taken over by the thieves, preventing much more extensive theft. It is not clear that as a target #4 could have done anything to prevent this theft, as the operation was a highly sophisticated international hacking effort taking place online, and hacking into a broker data bank and his theft was among thousands of personal identities stolen in the operation (at the same time, the size of these operations also greatly increases the chances of notification occurring in short order). Nonetheless, rather cryptically, #4 reported that he had personally been under criminal investigation because of the compromise of his data, which indicates that it had likely already taken more than a year to resolve. Though it appears that it took some time to resolve, other than the investigation, #4 clearly took protective action, likely closing and changing accounts, certainly being issued new credit cards.

Victim #t#5

It has been 3 years since I retired to the Caribbean. My house in New York was left unattended. I returned to put the house on the market because I don't have a need for it here. When I consulted my real estate agent, she notified me that the title to my house was under

someone else's name. My lawyer found out that an illegal alien from Mexico took my personal information including my name, bought a car, took possession of my house with forged papers and moved into my house with his family. One of his children is going to college under my last name. When I went to Department of Motor Vehicles to renew my license, they called the police because they told me that I received my license under somebody else's name. I spent one night in jail and have been going back and forth to court to clear my name. Now I am a victim of the government system. My lawyer gave me a letter with his name and number and told me that I should carry it on me at all times just in case I get stopped by the police. My wife is in the hospital because of this mess. I cannot event get a credit card right now. I must wait for my lawyer to help me clean up my credit. I feel very embarrassed and helpless because of this. I don't know which way to turn any more without looking over my shoulder.

Analysis of #5

Once again, #5 is a retire, and was living abroad. He only became aware that identity fraud had taken place with his personal ID when he returned to New York, presumably after a year or so, and found that an illegal alien from Mexico had stolen his data and used it to set up a legal life in the U.S. using a false ID to get a driver's license, buy a car, put a child through college and even take possession of the victim's vacant house! This is classifiable as a highly viral example of identity fraud resulting in taking on another person's identity, generally found to be rare. He only found out about this theft, not through any red flag or breach notification law, indicating that the thief was modest in his illegal credit card use to protect a false lifestyle, by his real estate agent reporting that his house was in someone else's name (it is not clear why this would not have been noted earlier). #5 is quite explicit in defining official response to his

situation as revictimisation. The problems started in government offices, the Department of Motor Vehicles, where, generally, paperwork is interpreted as reality. When they determined that #5 was applying for a license that was already in existence under another name, his guilt was assumed, and police were called. The police actually placed the victim in jail overnight, and #5 had to go "back and forth" to court to clear his name. The experience has left him permanently distrustful as "a victim of the government system" to the extent that, on the advice of counsel, he even carries extra identification on his person at all times to prevent any police stopping from again putting him in jail. The lawyer continues to try to clear his credit problem, until then he cannot apply for a new card. His wife was hospitalized due to stress and he espoused a feeling of embarrassment and helplessness—and a permanent suspiciousness over the system. There is an implication, from a retired home-owning Puerto Rican-American who had lived for a long time in the U.S., of racism in the attitude toward re-victimising government response. Once again, it appears that standard operating procedure among clerks of government offices, police departments and credit card companies is that paperwork is reality and the victim is guilty of fraud until the situation is cleared by a lawyer. From his comments, the whole process of resolving the problem appears to have taken years. Again, an emotional sense, characterized by shock, at double victimisation, focused the interview on this aspect of his case, meaning that #5 did not provide answers to all research questions.

#6

When I was nineteen years old I went to the cell phone store to buy a phone. They told me that they could not give me a phone because I already had one. Even though I told them that I did not have any credit under my name, the manager at the store showed me a credit report with

my name, social security number and a date of birth of a 35year old man. I even saw the man's photo ID card that he left on file at the store. I could not get a phone at the time and the police were called. They searched my pockets and I felt like a common criminal. When I objected to the search, one of the officers pushed me, slammed my shoulder against the wall and told me that if I did not follow their commands I would be arrested, no questions asked. The impostor bought a car under my name. He even paid his social security under my name for ten years although I was too young to work at the time. It took approximately 6 ½ years to restore my credit.

Analysis of #6

#6 was a 19-year-old young man who did not even have a credit card yet, but whose identity had been stolen for the purposes of creating a false credit card to buy numerous goods. He only became aware of the theft when he went to a store to buy a phone and was told that a phone already existed on that account, with the store even showing him a picture of the fraudster on file. This means that the phone company store accepted the fraudulent card at face value without any further ID checking. The dollar amount for the phone was no more than $600, but the fraudster also used the card to buy a car under #6's name, and pay his social security from work. The time-frame involved in this crime was extensive, the fraudster had been paying into social security on the victim's number for over ten years, it took the victim over six years to clear his name and restore his credit. This then again suggests, as with Barbara, that identity thieves may target youth because they will not become aware of the crime for years. It was not clear how his identity was compromised, and, certainly, he could have done nothing to prevent it as he had no target behaviours with regard to data use. Here, again, the phone company involved acted

as if paperwork were reality, in essence, accepted the fraudulent account as real, assumed that the victim was a fraudster, called the police, the police treated him “like a common criminal” and, when the victim objected, even were forceful with what they viewed as resistance of arrest and threatened arrest, possibly escalating the crime against him into a crime committed by him (resisting arrest). #6 clearly, then, characterized both company and police response in the framework of revictimisation. The interview was full as #6 covered all of the questions; being youthful, he seemed more nonplussed than emotional over his experience with identity theft.

#7

I fell victim to ID theft 7 years ago. Credit card companies are still calling and notifying me that people are attempting to use my identity. The debt collectors keep harassing me about unpaid credit card and utility bills. I still receive letters informing me that people out there are still trying to get hold of my password because they want to get into my personal account. Someone recently tried to order checks in my name. They don’t care if they ruin my life. I was advised to register with the FTC website to get the help that I need and that I can keep track of what they are doing. This is a full time job in itself. I am frustrated but there is not much that I can do. Two people got arrested for damaging my name. None of them served prison time but I am the one left holding the bag.

Analysis of #7

#7 only provided a highly partial view of his identity theft situation, focusing almost entirely, and with a sense of amazed, helpless shock, at how long it has taken for the identity

theft against him to go away. Seven years after having his identity stolen he still receiving calls from credit card companies, debt collectors, breach notification agencies, red flag agencies, and banks, both still insisting that he is responsible for the fraudulent credit card use made against his account (presumably now closed), that he is responsible for the fraudulent bills run up with stolen cards (accounts presumably now closed), and that, apparently, his ID continues to be compromised, having once been compromised so long ago. He described efforts to fight off these solicitations and to monitor his financial life as itself a full time job. Still he directed most of his anger at the original thieves whom he characterised as not caring if they ruined his life. #7 did not report any direct revictimisation by law enforcement but was unimpressed with law enforcement response, dismissing as a wrist slap their arrest, without prison time. Indirectly, then, he is left frustrated and "holding the bag," that is, in the end, #7 himself as a victim who had not received any redress for the crime against him.

#8

Credit bureaus have notified my family as recently as a week ago that someone tried to apply for new credit cards from American Express and Saks Fifth Avenue in our name. The telephone company called and sent us harassing letters notifying us that our service would be disconnected if the bill was not paid. There is a current case in court with a gang of thieves who did this unspeakable act to us. The prosecutor gave us a letter to send copies to companies that we do business with if there is a problem. The prosecutor notified us that this could take up to seven years to turn around.

Analysis of #8

#8 did not identify him or herself demographically, but became aware of the credit card fraud using his number through a credit card company acting on a red flag rule and breach notification law protocol. The fact that the red flag was raised within a week or so of occurrence is a positive sign. In some way, however, the credit card fraud resulting in illegal phone bill accounts being set up, and then not paid, resulting in threatening phone calls from the telephone company, to cut off service. This indicates that the telephone company has no mechanism in place to discern the difference between legitimate and fraudulent account creation and credit card use. It also indicates that, like all other bill-collecting stakeholders as recorded in other case studies, telephone companies operate under the assumption that all the data they work with is legitimate and not fraudulent. The client was aware of the fact that a gang currently involved in the court case may have been to blame for the crime, but did not express a great deal of certainty about this or any view as to the kind of punishment they would receive. It is not clear what the total dollar amount suffered was, negative outcomes other than the theft were not indicated. #8 likely had to close the credit card accounts that had been compromised, but did not indicate this directly. They seemed grateful that the prosecutor of the gang identity theft case provided them with a document proving that they were victims of identity theft which they could send to any debt collector to explain their situation, but generally seemed unimpressed by the criminal justice response to the crime. They characterized the crime as “unspeakable,” indicating trauma. #8 seemed incredulous that, as indicated by the prosecutor, it would take up to seven years for the after effects of the identity theft to go away, but testimony from other victims have confirmed this figure generally. No mention was made of police response.

#9

My husband was a victim of ID theft. Last Memorial Day weekend we packed up the kids and were on the Jersey turnpike heading to our family reunion in Virginia. We were pulled over by the police and waited at the side of the road for about 15 minutes. My husband attempted to get out of the car to ask the officer why we were pulled over. We were told to stay in the car. The kids started crying when another police car pulled in front of us. My husband was instructed to step out of our car, put his hands in the air and don't move. The officers put handcuffs on my husband while the kids were screaming and told me that my husband was wanted for a murder in South Carolina. He was taken away and spent two days in jail before the courts realised that my husband was innocent. My husband lost his job and found out that his credit was damaged because someone applied for a duplicate social security card, driver's license and credit cards in his name.

Analysis of #9

#9 provided only a partial, highly emotional account of the impact of identity theft of her husband's credit card numbers, as well as the creation of a false identity with duplicate social security card numbers and driver's license numbers. It is this dimension of the crime of identity theft that precipitated contact with police, the overwhelming subject of #9's response. Undoubtedly, the false driver's license created with the stolen identity had attached some negative activity to it, possibly ranging from unpaid tickets to moving violations, which caused the actual license plate of the real person, whose identity was stolen to be flagged, causing police to stop him. It turned out that the identity fraudster who operated a vehicle with a driver's

license manufactured from his stolen identity was wanted for murder in South Carolina. For this reason, the victim was apprehended, put through the rigours of arrest, and taken to jail where he spent two days before the courts finally realised that this was a case of false arrest due to identity theft. It is implied that, as an after effect of this incident, the victim also lost his job, though it is unclear if his employer fired him because this arrest went on his record, which would constitute a non-arrest on an un-real record. Needless to say, the victim's credit was destroyed. It also goes without saying that in recounting this incident, in a highly emotional way, focusing on the trauma presented to their children, for example, #9 had nothing but amazed contempt at the rigid paperwork-is-truth way that police had in dealing with the situation, never at any point in their proceduralism acknowledging that identity theft may be involved. This again means that they operate without any training in detecting anomalies between records and persons, or any sort of confirmation of red flags in arrest situations, and even perhaps operate innocent of any consideration of the possibility that the data systems they work with to flag down criminals may be corrupted by identity theft. It is likely that in this case, in which false arrest occurred, the husband has a legitimate lawsuit against the New Jersey state police. As so often happens in emotional victim response, usually focused on the most important fact of dealing with identity theft, no mention was made of what preventive actions they subsequently took, or how long it took for resolution. If the husband remained unemployed for some period of time, all of that time would have to be considered part of the time-frame of getting over identity theft. Finally, it was not clear how the husband behaved as a target, and how his identity was stolen in the first place.

#10

I am a Senior VP for a leading financial company in Wall Street and never had one iota that I was vulnerable to financial scams. I received an email from what I thought was a legitimate Microsoft website requesting that I update my personal information or my email connection will be permanently revoked. I continued to ignore the email until one day, I received the final notice. Little did I know, it was a fraudulent fishing email? I took the bait and responded with information on my full name, social security number, date of birth and father's middle name. A day later, I received emails from several people in my email address book. Everyone wanted to know if I was missing an arm and needed $3000.00 for surgery. When I examined the fraudulent email I realised that my account had been hacked and everyone in my email address book received the same message. It took several weeks and a few hundred dollars working with a tech support firm to clean up my email. I have lost two days from work attempting to have my email and contact list cleaned up and recovered. This included changing my password for important things such as banking, medical and other financial entities that I am associated with throughout my daily life. This has taught me a lesson on how not to give in to phishing and other email scams on the Internet.

Analysis of #10

#10 focused on the manner in which his identity stolen, perhaps out of embarrassment that as Senior VP in financial management he should have known better not to "take the bait" and fall for one of the most common new kinds of means of identity theft on the Internet, phishing. His stance before the incident was that he would never be susceptible to identity theft, a view that must be classified, even for professionals, as naive. In his case, he responded to a

communication from a dummy website with a request for clarification or update of information: what he should have done was not respond. But he responded. He found out fairly quickly, within a day, that he had made a mistake, when several friends on his list of emails emailed him asking him if he had lost a limb overseas and was in dire need of direct funds for surgery. This meant that the fraudsters took his information, hacked into his email address book, and then sent a typical emergency-need email to all of his correspondents, hoping to exploit them for either more identity thefts or money. Fortunately, this happened quickly, he immediately realized his mistake, he involved a tech support firm connected to his work place in cleaning up his email, but it still took him up to two weeks and a few missed days of work to clean up the mess and restore his email contact list for business purposes. This, then, is an example of a suitable target behaviour that consumers must be trained not to respond to, in order to reduce the incidence of phishing. #10 had to learn the hard way, though, because of his status and his support structure at work, damage to him, a matter of a few hundred dollars, was minimal. He changed his password for all important transactions online, though did not appear to feel the need to close accounts. The fact that he had in-house support, that the problem was taken care of expeditiously, and that the amount lost was minor, not only minimized the sense of victimisation, but meant that law enforcement was not involved. This latter point might be good thing, but could also work to reinforce the corporate sense that they can take care of the problem themselves. It would appear, in analysing the case, that the lack of sophistication of the scheme, and the fact that #10 had a number of highly suspicious email colleagues who immediately questioned the validity of the false email and therefore contacted #10 limited the damage. Had they pursued a more sophisticated use of stolen data that would not have come back to #10 sooner, the damage, for a

Senior VP with considerable assets, could have much greater. This is a cautionary tale on the target side of the routine activities theory equation.

#11

I received an email from a lawyer in London notifying me that a distant relative passed away and left a substantial amount of money for me. Even though I did not know my relative, I replied to the email asking why me? I was told that my relative did not have an offspring to whom she could leave the inheritance. The lawyer further requested my bank account details and further stipulated that if the 1 million pounds sat in the bank much longer that it will be awarded to the state. Needless to say, I panicked, forwarded my bank account information. After a few days, I emailed the lawyer several times and got no reply. I thought it was best to move on with my daily life instead of waiting to receive money that I previously knew nothing about. Three months later, the debt collectors were calling my house every day inquiring about funds owed to various companies, such as, utilities, electronics, and financial institutions. I then realised that I might have been scammed by the letter from the lawyer in London. This caused me to change my phone number and my address. Some $30,000 was drawn out of my account electronically and I continue to live the nightmare. When I consulted the police, they told me that there was very little that they could do about this kind of crime because the criminals were probably overseas somewhere.

Analysis of #11

11 described himself as a businessman, who, again, unwisely responded to email correspondence that turned out to be phishing. His response was lax, in that after initial contact, he, in fact, provided a law firm in London with personal data by email, then, after receiving no response in three days, let it go. It was only three months later that he began to receive phone calls from debt collectors every day, telling him that he owed money on utilities, electronics, financial services, that he put two and two together and realised he had been scammed. That is, he was not contacted by his own credit card company or bank based on red flag or breach notification rules, but by debt collecting acting on the debt incurred by the fraudster who stole his data from an overseas location. The total dollar amount that he lost was substantial, $30,000. As of the interview, the problem had not been cleared up, with #11 characterising his situation as continuing to "live the nightmare." To clear up the problem he changed his email address and his phone number, which may not be classified as best practice. The phishing email that he responded to is the kind of thing that any consumer training based on routine activities theory attempts to reduce target suitability might have warned him of, especially as it exploited a kind of urban legend. That is, he was an American victim being told that he had inherited a fortune from an unknown uncle in the UK and that if he did not respond with personal data to claim it immediately it would revert to the state. It is likely that he "fell" for this scam precisely because it is based on a scenario endlessly repeated in movies over the past 75 years. As with #10, #11 spoke with a regretful tone in his testimony, as if he should have known better: and he should have. As to his comments on the guardianship aspect of the equation, his refrain was common; he was told by the police that they could do nothing because the crime, having been committed overseas, was outside of their jurisdiction. #11 at least did not report any re-victimising behaviour by the police.

#12

I received a disconnect service notice for my gas and electric bill and chose to ignore the notice because I knew that my utility payments were never paid late or left unpaid. So I decided to ignore the notice until one day, as I arrived at home there was a final disconnect notice on my front door. I laugh at the notice and called the utility company. The customer service representative transferred me to the collections department. I was told that I owed an additional payment for utilities at another address that I was not familiar with. When I requested a faxed copy of the outstanding bill, I noticed that an account was opened in my name at another address. This account was opened for three years using my name, social security, and drivers licence. Furthermore, an automobile was bought in my name along with credit cards. It has been very difficult for my family and I knowing that there is an impostor lurking out there using my name for their financial gain. I have enlisted the help of an attorney and the police to correct the situation. However, the investigation is moving at a snail's pace and it has become very frustrating for my family to deal with.

Analysis of #12

#12 was also a business person, with no history of credit or bill-paying problems. He was also the victim of full-scale identity theft fraud, in which his personal data was used by the fraudster to set up a phony identity making use of a host of credit cards and services. He only heard about the identity theft indirectly when the gas and electric company notified him of a disconnection of service, even though he considered himself up to date on his payments. As a result, he ignored the notices until a final disconnect notice arrived. Only at that point did he

contact the company, at which time the collections department informed him that he owed money on another address at an unknown location where a fraudster had opened an account. Upon further investigation, #12 found out that the fraudster had also created a false social security card, a false driver's license and even bought a car with false credit cards. This had gone on for three years. It is unclear why these broader infractions, emerging in victim responses as a common phenomenon, were not flagged earlier. Apparently, the gas and electric company would not accept his testimony that fraud was involved, and, one imagines, his credit card companies also were unresponsive, as a solution to his problem required hiring an attorney, and involving the police. His comment on police involvement was that the investigation is moving at a snails' pace. As for broader impact, #12 only mentioned that the situation was been very difficult for his family, noting that the knowledge that someone is out here as an impostor has haunted it, and he described the ongoing, unresolved situation as frustrating. #12 provided a more or less full interview, answering all questions relevant to the research questions.

#13

My bank account was compromised almost 7 years ago. The problem started when I went to an ATM machine for a withdrawal. The machine ate my card and I left it in there. The following morning I contacted the bank and was told that someone had placed some kind of device on their machine. When customers inserted their cards, the machine swallowed all of the cards and the thieves took the cards and then made other cards from the originals. Over $45,000 was taken from my account but the bank reimbursed my account. I did not lose anything at the time. The bank also paid for all of the customer's credit to be monitored for 1 year. However, I continue to be notified by the credit agencies that unknown individuals are attempting to access

my credit files. I have also received notices from department stores whenever the thieves attempt open credit in my name.

Analysis of #13

#13 had a bank account and so it must be assumed that he was employed and had assets to steal, a common theme. He discovered the theft after one of the most common scams, fraudsters manipulating ATMs to eat cards, the extracting the numbers that on. Because this is clearly a problem of bank security, the bank, which is insured, reimburses any such theft, but their oversight ends with that, and in this case the number was then used for other fraudulent purposes. In terms of notification, then, this was a two-stage crime, first notification was quick and easy, but then credit agencies began to call #13 to inform him of suspicious activity on his accounts. He also received notices from department stores when thieves tried to open accounts there. There is the suggestion that in both cases a red flag rule caught suspicious activity before any more damage could be done. That said the total amount of this crime was not insubstantial, $45,000. The fact that he continues to be contacted by these companies of further problems indicates some failure to cut off the use of the fraudulent number. This continues to occur after seven years. Thus, because of the on-the-street manner in which the original theft happened, bank oversight was immediately brought in, not only was the bank forced to reimburse him but monitored his account, and, it is inferred, contributed to a system of monitoring that involved being notified by credit card companies and stores, but according to red flag rules and not as debt collectors. Nonetheless, it remains disturbing that thieves continue to present the stolen number to these locales after seven years, suggesting that they are trying to out-wait the monitoring. By

and large, #13's case study exemplifies the benefits of an ID theft that occurs within a bank context.

#14

I was at my office one afternoon when I was contacted by a lawyer acting on behalf of his client with whom I reneged on an auction deal. The lawyer informed me that I made a bid on an artefact worth thousands of dollars. Soon thereafter, a savings and loan company sent letters for non payment of a mortgage and the creditors were calling for debts on which I had defaulted. This has been an ongoing nightmare for me. I even had to enlist the help of an attorney to figure out this financial mess caused by unknown fraudulent activities. It is a continuous situation and I am unable to place a dollar figure on the damage caused by scammers. This has cost me thousands of dollars in my quest to undo what was done to my family name.

Analysis of #14

As #14 reported that he was at his office when he found out, this again indicates a gainfully employed professional as the target. One day a lawyer working for an auction house contacted #14 to collect a debt, as the fraudster had purchased an artefact at auction. This means that #14 did not know that his identity had been stolen, and it was several months until he became aware of it. This was the first of a series of notices, including those for defaulted mortgaged and credit card debts, indicating that after the initial scam the fraudster had made extensive use of the stolen ID to set up a lifestyle. The artefact itself was worth several thousand dollars, the other bills conceivably equalled or surpassed that amount though #14 reported being unable to place a dollar figure on the total amount, though in addition to that it cost him

thousands of dollars to clear his name through lawyers or other channels. In terms of time frame, it was still ongoing, and was described by #14 as an ongoing nightmare. #14 provided a fairly full account of all relevant data about his identity theft experience.

#15

I was unemployed for 18 months. One of my daily routines was to surf the net for job openings. I needed a job in tech support. I answered an ad for a tech support engineer. After emailing my social security number, date of birth and address, I was told to send $25 for a processing fee. The $25 was wired from my wife's account. A few days went by and I heard nothing. When I called the telephone number that was associated with the job offer, the number was no longer in service. I realised that I had been had. This left me dejected and depressed. I am now seeing a psychiatrist to help straighten my life out. The financial companies keep calling my wife and me telling us that we owe then money for bills that I am not responsible for. Now the Attorney General's office is looking into this scam.

Analysis of #15

#15 was unemployed for a time, but a technical engineer by profession. As part of his job search, he responded to want ads or other job search site entries, as part of his job search. He was not aware that there was any danger in this practice, or that he had had his identity stolen by one of these sites, which must have turned out to be phony. It was only some months later when, as in so many other cases, he was notified by credit card agencies that there was suspicious activity on his account. Once again, then, red flag and breach notification rules occasioned first contact with victim. He also received credit notices from department stores, also in the nature of red flag and breach notification rule responses. In both cases, then, the credit card companies

and department stores were acting an in an informed way, and not in the manner of a debt collector. As a result, financial companies appear to be less informed, as they continue to call both #15 and his wife, claiming that he owes them money based on fraudulent purchases by the scammers. Again, the fact that a financial company would act in this manner is somewhat surprising. As in so many other testimonies, #15 reported that having his identity stolen and being victimised in this manner left him so depressed that he had to seek out assistance from a psychiatrist to "straighten out his life." With regard to routine activities that made him vulnerable, while it perhaps not feasible to stop persons from looking for work online, the fact that a site asked #15 for personal information, and he complied, that he was asked for a processing fee in advance for $25, and he complied, and that he wired the $25 from his wife's account, thus providing still more personal data, all must be classified as ill-informed and naive responses that a simple awareness program might have helped #15 avoid. Moreover, even before the onset of the age of the Internet, it has been a well-established precaution that any solicitation asking for personal data or, more tellingly, payment up front, before delivering services, is not to be trusted. Perhaps because an undercurrent of embarrassment that he had fallen for this scam #15's interview was not entirely complete, with limited detail on defensive action, apart from changing his behaviour, he undertook in response to the theft. Finally, #15 did not appear to go to law enforcement for help, but the scam must have been widespread as it was subject to an Attorney General's investigation at the time of the interview. This seemed to allay some of #15's sense of helplessness at being victimised.

16

When I was contacted by a debt collector that I defaulted on a $17,000 credit card payment I told them that they had the wrong person because I did not own any credit cards and I never applied for any. This has taken about one year going back and forth and fighting with the card company and the debt collector to clear my name and prove that I do not own that bill. It is consuming all of my free time. I wish I did not have this nonsense to deal with but I have no choice. I must clear my name.

Analysis of #16

#16 only found out about his identity theft when a debt collector contacted him, informing him that he was delinquent in his payments. #16 argued with the credit company that he had never made such purchases. Insofar as this was the first time #16 was informed of the theft, and that the debt collection agency took the charges at face value and sought to collect based upon them, indicates that #16 became involved in the process of clearing his name by a method far from best practice. The amount total was high, again, as in all cases of businessmen, $17,000. The fact that #16 has had to fight back and forth with the credit card company and the debt collector again indicated poor practice, and greatly exacerbated the emotional stress of the event. In effect, both callers, credit card company and debt collector, neither informed by red flag or breach notification rules, harassed #16, and re-victimised him. This process consumed all of #16's free time, meaning that he chose to handle it alone (also not best practice). It also sounds like the back and forth turned his effort to undo the crime into a crusade as he mentioned clearing his name a few times. #16 was also so focused on his battle with illicit collectors that he gave no account of additional defensive action he had taken. He never became aware of how his identity was exposed, or how it was stolen. It is not clear that #16 even fully recognized what

had happened to him. #16's case study is a textbook example of the complications and unnecessary trauma that results when debt collectors bring their motivation into the scenario as well.

#17

It has taken me 16 months, long hours on the telephone, attorney's fees, convincing the police that I am not the one who defaulted on a $10,000 debit and maintaining my sanity. I am going out of my mind dealing with what other people who don't want to earn an honest living have done to me. Something has to be done very quickly if not we will all be victims of these scams. How do they know who to pick on? And what are the politicians doing about this?

Analysis of #17

#17 likewise was only informed of the fact that he owed an unpaid debt by a debt collector and as a result spent long hours over the course of 16 months trying to clear his name. This process involved having to involve and lawyer. The total amount was about $10,000, again not insubstantial. He mentioned having to convince the police that he was not the fraudster, meaning that he was re-victimised by their lack of awareness of the crime. Again, because of the ill-informed response by all stakeholders involved, the effort to clear his name has caused #17 considerable stress and emotional upset. #17 also overcast his recounting of his experience with a doomsday scenario and a sense of outrage and injustice at the fact that identity thieves seem to operate with impunity. When it came to politicians, #17's tone became more frustrated, and somewhat helpless. Because #17 was so fixated on the trauma of clearing his name, undoubtedly frustrated by the manner in which he chose to do this, he provided only a partial, highly emotional response which did not cover more practical points in terms of defensive actions. It is not clear that he ever came to understand what he might have done to expose his identity to theft.

#18

My home was burglarised by the neighbour's gardener. He stole personal items including my credit cards along with my vintage Porsche. The following day, police stopped the car and found a burlap bag containing lot of credit cards, driver's licenses from other states along with my mail that was delivered on the day that my home was burglarized. One week later, I received a call from an auto dealership asking about the extras that I ordered for the interior of a new car. I

also received a visit from a detective who wanted to know why I did not make my payments on an account at a furniture store. When I enquired further, I was told that I had taken out $22,000 worth of furniture on credit two months prior. I was angry, frustrated and shamed because the neighbours knew that the police were previously looking for me.

Analysis of #18

#18, a Porsche-owner, is clearly a successful businessman. He experienced a crime, which appeared to be “traditional,” then found out that it also involved the newer dimension of identity theft. The original crime was theft of goods from his house, in addition to that Porsche sitting in the driveway. Thus, a substantial amount was already involved. But about a week later #18 received a phone call from the auto dealership asking about the extras he had ordered for the car. Is it possible that the thief took the stolen Porsche to #18’s dealership to order extras installed using #18’s stolen credit card? It seems so: but it also appears that the dealer knew #18 so made the call. At the same time, #18 received a visit from a detective working on behalf of a furniture store, collecting payment for purchases. This too was a credit card purchase, and of a substantial amount, $22,000. Therefore, the fraudster was building a lifestyle for himself on #18’s identity. Needless to say, #18 was angry, and also frustrated. It also appears that, relevant to police involvement, they had inquired of #18 with neighbours, and had been “looking for him “for some time: it is not clear how or why they were involved in this way, presumably investigating reports of what stores might have presumed was fraudulent activity. The fact that the police proceeded in this fashion was a point of considerable embarrassment to #18, which he characterized as shame: an emotion signalling a sense of revictimisation. The time line for the

police involvement is muddied still further by #18's report that his stolen Porsche was found within 24 hours of the theft, and that a bag filled with stolen credit cards, including one piece of his, mail was in it. And yet it appears that he only was notified a week later. #18 seemed most upset by the fact that the detective came to his front door and did not call him down to the police station, indicating his social status and his concern for it and his name. It is obviously not clear what #18 might have done to prevent the theft from happening, except perhaps to collect his mail as soon as delivered, or dispose of it or process it as soon as received, and not leave credit cards lying around the house. Usually, rich man's houses are so enveloped in security that as a target they present too much of a challenge to thieves, so there is a missing link here; it does appear that #18's security was lax. While it could be said that the investigatory arm of the police department acted more or less in a forthright manner, there are some details which suggest less than best practice. Still, it does appear that the only element of this crime that reduced its magnitude was the thief's stupidity, which, perhaps, one cannot always depend upon (though the involvement of street criminals in an identity theft cycle may bring that into the equation more often than not).

#19

I started getting notices from creditors about my information being used for multiple purposes. I then realised that Macys and the Home Depot stores had accounts in my name without my permission. I knew it was time to fight back but fighting back was not that simple. An illegal immigrant from Guatemala and the whole family was using my name for work purposes. I called the local authorities and they told me that it was a common thing and that Immigration reform is needed to fix this problem. Why should I have to wait for the President

and Congress to pass an immigration bill to help these impostors and all the while my name is being dragged through the mud? It is not fair to me as a victim. I get very angry at times. Unless something is done to correct the situation more lives will be harmed by these thieves.

Analysis of #19

#19 is still another case of a person only finding out that his identity has been stolen by receipt, sometime after the fact, of notices of bills not paid by creditors, including department stores. The fact that #19 did not have accounts at either of the department stores alerted him that this was more than confusion. Once again, the fact that these notices were not in keeping with red flag or breach notification rules, but simply to collect a debt, regardless of who incurred it, represents poor practice, and, once again, this incidence appears to have backed #19 up into a highly defensive fighting mood to clear his name. Only later did #19 come to find out that a family of illegal aliens from Guatemala had stolen his identity and used it to set up a 'legal' lifestyle in the U.S. even using his name to gain employment and collect social security. This is a recurrent theme, but, more generally, again indicates that, while the research did not overly focus on this dimension of identity theft, building up a false identity with full false documentation is one of the major recurring motivations for identity theft as testified by respondents. #19 was not overly impressed with law enforcement response. Local authorities, presumably police, told him that this kind of fraud by illegal aliens was common and that, in effect, there was nothing they could do about it until immigration law was changed to fix the problem. The combination of inopportune informing of #19 and the sense of impotence by law enforcement combined to create a considerable degree of anger in #19, whose response must be characterized as partial due to emotion. Again, as in other poor practice cases, #19's anger found

expression in calls for Congress and laws to stop the problem. #19 clearly espoused views that indicate both victimisation and revictimisation, that is, something was being done to him, then nothing being done about it.

#20

A ring of illegal aliens somehow got hold of my personal details and was using them to get places to live, to work and take out credit. I received a letter in the mail asking me if I wanted to refinance my home in Plano Texas. When I contacted someone at the savings and loan, they told me that my house was ready to be refinanced. I told them that they had the right name but the wrong person. When I ran my credit report, I realised that several individuals were using my personal information to hide in the United States. There were outstanding bills for several thousands of dollars attached to my name. It is not a good feeling. As a victim, I felt alone, left out and violated with not many places to turn to.

Analysis of #20

#20 was again a case of identity fraud where illegal aliens were involved in using ID to set up a false life in the U.S. Here too #20 only found out about the ongoing crime when a savings and loan company naively called him and informed him that his house was ready for refinancing, meaning that the savings and loan had taken the fraudulent activity provided them at face value, and had in place no red flag or breach notification rules for a client of theirs. At this, #20 ran a credit report, only at this point seeing the extent of the credit damage done to him by the fraudsters. The amount of the crime was measured in thousands of dollars, but if a house refinancing was also involved, this was a major crime. #20 expressed the notion that no one

helped him to resolve his situation, leaving him feeling alienated and isolated. The fact that the home refinancing was occurring in Texas, when he did not live there, meant that the crime was outside of police jurisdiction. Though muted, #20 did not express any positive feelings about the capacity of law enforcement to help him resolve the issue. He did not mention how the savings and loan resolved the issue.

#21

I stopped by my bank's ATM on my way back from vacation, and as I checked my balance, it said I was overdrawn by $200.00. It kind of surprised me a little bit; I've never overdrawn a bank account. I immediately panicked, and I went into the bank to see if I could figure out why I was overdrawn. Of course, I felt like everyone was judging me because my account was overdrawn, and everyone was kind of rude. I requested that they print out my statement, which I looked over trying to figure out where I messed up. I saw that the $200.00 was a charge from place called Fifth Avenue which I have no idea where this is or neither have I been there. I explained to the bank teller that I didn't make the charge. She went to fetch her supervisor who told me that I would have to go through a formal process to investigate it, and that could take up to two weeks. Not only will I have to wait that long after filing the complaint, but the bank will continue to charge me overdraft fees until they were able to confirm that it was not my fault! I left the bank in frustration, and I went home. The next morning, I pulled my credit report, and I found a couple of accounts on there that weren't mine, a Nordstrom's store card and an AmEx card, both of them were maxed out. The Nordstrom card has $5,500. 00 and the AmEx card $7,000.00. I never applied for either of those cards. How could this have happened without my knowing? I called the police department to file an ID theft report while I gather enough

information to contact the creditors. It was a long and stressful fight and even after three years, I am still dealing with the residue of my identity being stolen.

Analysis of #21

#21, again, coming back from vacation, was an employed business person, who sounds like he keeps very careful watch over his financial life, if he was aware of and upset by the extraordinary occurrence of a $200.00 overdraft. It is a small amount, it sounds like it took about two weeks to find out that the crime had occurred. He felt like the bank was unhelpful and judgemental, suggesting that the bank had not yet implemented standard identity theft insurance and security policies. Nonetheless, receiving a print out, then showing an unexplained charge to the teller is good practice on #21's part. The fact that #21 had no idea where Fifth Avenue is again indicates that he is not a sophisticated consumer. At this point, however, the bank informed her that they did have a standard reimbursement procedure, but that it would take up to two weeks. #21 was also upset that she would be charged for overdraft in the interim. Though this cannot be considered ideal policy, and is rather unfriendly to clients, it is in accordance with current bank best practice: only in detected rudeness and assumption of guilt by local branch bank tellers was best practice breached, as the assumption is that the bank will reimburse. But #21 did have credit cards, a credit report, and the next day, revealed a much larger amount crime, amounting to almost $10,000 of charges at department stores where #21 did not have an account, and possibly could not even afford, given response to a $200.00 overdraft. This is when the crime of identity theft escalated far beyond #21's level of awareness as she expressed incredulity at how department stores could accept applications without some other substantiating proof of identity (which also means department stores may not have good red flags and no breach

notification law liability). #21 reported that this part of the crime is ongoing, in terms of clearing her name, and has taken up to three years. While she filed an ID theft report at the local police department, she continues to engage in information gathering to take on her creditors, whom, it is presumed, continue to harass her as if the fraudulent bills are hers. #21 seemed to reserve most of her complaint for the bank, perhaps evincing an attitude that they are responsible for more oversight of credit card activity as well. She had no great confidence in police involvement, and, indeed, in most cases, police reports are not required in bank reimbursement procedures and apparently do not help much with creditors either. #21's responses were fairly thorough, covering most points of her incident.

#22

I heard my doorbell ring and walked briskly to the door on a beautiful Saturday morning. Standing there at my door was a detective and the police to ask if I were the guy they were looking for. After showing them my ID, they told me that there has been an arrest and that a woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. And it happens that I am the victim! My whole world stopped and I could not say anything but give them a blank stare. I was lead to the police station to file a complaint, and I also hired a lawyer to clean my record. It is a very agonizing to have your credit that you've built for many years wiped by an impostor. This person going to jail did not stop me from building back up my credit. You would think there will be a law that would help people who are victims of identity theft.

Analysis of #22

#22, again a middle class home-owner, represents a rare case where first notification of the crime to a consumer is provided by a police detective reporting that after an arrest, investigation and prosecution of an ID theft fraudster, her name was found to be one of the victims. By this point, the extent of the crime was considerable, involving thousands of dollars of credit and a filing for bankruptcy under her name. Whether or not police arriving at a victim's front door represents best practice is a matter of debate, #22 responded with shock, indicating not only lack of awareness of identity theft, but astonishment in how the message was delivered.

#23

My wife and I moved into our new home, and requested that the US postal services transfer our mail to the new address. However, some of our mails still got delivered at the old address. The new tenant opened some of our mails and got a hold of our private bank account statement of our insurance policy and used the information to deposit $479.000 in counterfeit checks into a bank account that he had established. I was told to contact The Federal Trade Commission (FTC) to report the situation, and file a complaint as well with my local police. The person was arrested but I will have to live with this on my record for a long time.

Analysis of #23

It is unclear that #23 could have behaved in a way that might have avoided the crime as it is unlikely to be expected that the U.S. postal service will be completely successful in responding to a change of address form, resulting in old mail with personal data enclosed being sent to the old address. It is also not to be expected that the new resident would then commit a crime and

make use of this data for ID theft. The size of the crime, $479.00, was not great, but shows recklessness and lack of professional street smarts, indicating an amateur exploiting an unexpected opportunity. It does not seem likely that involving the U.S. Postal service as well as new occupants at old residents in a protocol of consumer training would be practical: in other words, this is an unusual pathway to crime, which #23 cannot be faulted for. #23 reported going to the police, filing a report (mail theft would be in jurisdiction), hiring a lawyer to handle problems with credit card companies, but ended up expressing amazement that laws seem lax or non existent in prosecuting identity thieves.

#24

A ring of thieves bought expensive cars, houses and jewelry and auctioned the items with fake titles in my name. They then flew the coop overseas to England, Nigeria and Lebanon taking the money that was transferred through the banks in New York. My credit report reads like a will. I am not sure if I will be able to ever repair the damage that was done to me. They left me being responsible for over $2 million dollars. It is very confusing to me that the authorities in this country will let this kind of thing fester and injure someone’s name and livelihood. I tried applying for a new social security card and identity but it is not as easy to do. I need a politician to help with this.

Analysis of #24

#24 was by the far the largest crime discovered in respondent testimony, as his stolen ID became involved with an international ring that charged any number of illegal items around the world. The amount was more than $2 million, with the fact that his cards lead to that much money being taken out indicating that he is a wealthy individual. The fact that he mentioned "this country" in complaining of the police lack of response indicates a global businessman as well. #24's laconic description of his credit report is that it reads like a will. The fact that he is unclear how to apply for a new social security number, and that this a problem which requires a politician, perhaps also indicates the exploit-ability of foreign nationals of considerable means living in the U.S. Nonetheless, while confused by lack of law enforcement response, his level of trauma is not high.

#25

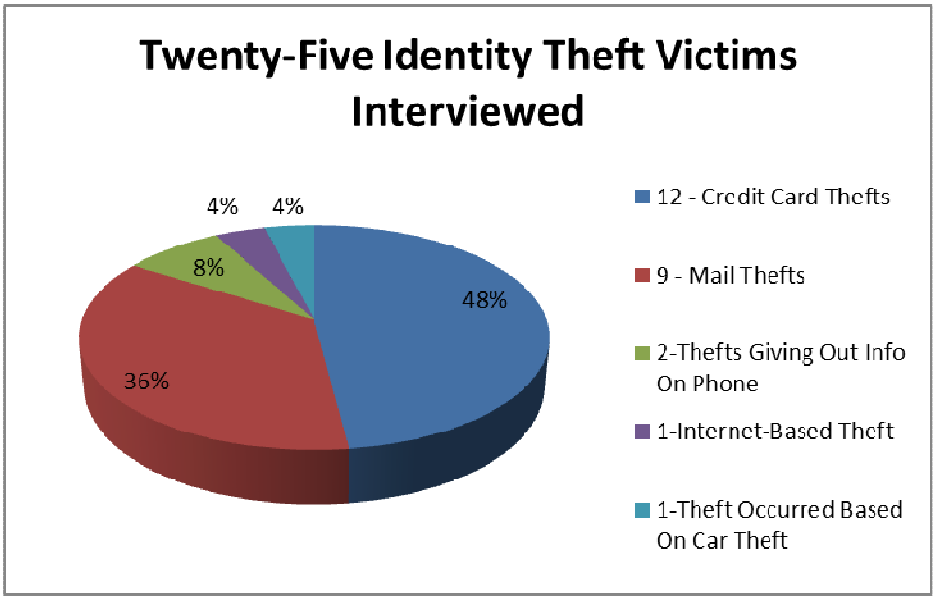
I suffered embarrassment, misery and the loss of all of my assets because my identity was stolen a decade ago. Bills were coming to my house for all kinds of merchandise and when I called the FBI they told me to contact my local law enforcement agency. They did very little to help and investigate the trail that was left from the bills that the thieves created. I even lost my husband when I could not convince him that I do not know what happened to my identity. He became suspicious and abusive and did not trust me ever again. I lost our home and am now living in a shelter. The damage is continuing because I don't know if I could ever get back my good name.

Analysis of #25

#25, finally, if she has been fighting to clear her name for over a decade, has been revictimised by the credit card companies that continue to harass her for fraudulent bills as if they were hers, and by inaction of law enforcement on all levels of government, with some evidence of passing the buck between the federal and local levels. The fact that #25, after a decade, still "does not know what happened to her identity," is, however, problematic. Also, the fact that he marriage collapsed because her husband was suspicious of her, frankly, raises a red flag. It is also to be hoped that after a decade, even with a home loss, some other means were at hand rather than living in a shelter. Overall, the lack of specificity about the nature of the crime, the similar vagueness about the time-frame of resolution, and the unclear nature of the extreme fallout of the crime on her personal life, all strongly infer that it may sometimes be difficult to discern a victim from a fraudster, still further complicating the picture of identity theft.

Of the twenty-five identity theft victims interviewed in this study, 12 had reported credit card theft, nine reported mail theft, two suspected that theft had occurred by giving out information on the phone, one reported internet-based theft, and one suspected that theft had occurred based on a car theft. An illustration of the percentage breakdown is shown below in table 7.

Table 7



*Note: The above table illustrates the methods (by percentage) used by offenders against the 25 identity theft victims who were interviewed for this study.

The findings indicate that victims' identities were compromised through the following channels. Victims reported that the primary place of compromise of their identity was through credit cards, a finding which corresponds to the research. The second most prevalent place of compromise was "unknown," indicating that the victims did not know where they lost the identity information, when it was taken, or by what means. This also corresponds to general findings that in large part victims often remain unaware of identity theft having taken place, until further compromised by subsequent fraudulent use of identity to withdraw funds from banks or use credit cards. The internet is the third most frequent site for identity theft, also indicating this growing trend, and the increased vulnerability consumers face as they engage in more and more activity on the World Wide Web. That mail is the fourth leading place of compromise means that mailbox theft, mail fraud, and, as mail is disposed of, consisting of bills or other personal data, dumpster diving remain popular ways for victims to be victimised.

The presence of restaurants on the graph is information derived from victims that was not recorded by either offenders or officials: victims appear aware of the fact that, perhaps in the use of credit cards at restaurants, combined with transient employees, or in the theft of unattended purses, or in coat check rooms, restaurants appear to be vulnerable places for the compromise of one's personal identity data. Other family members and military service were also recorded as sites of compromise, and family corresponds to research having found that offenders often gain access to private information through friends and relatives, but the incidence of identity theft in military contexts is unrecorded in the research. Overall, however, victim response to where they felt their identity was compromised more or less conforms to the research, indicating that, by and large, victims have a fairly high level of awareness of their current state of vulnerability.

(i) Analysis of Individual Testimonies

In addition to looking at the statistics, a summary analysis of the 25 victim testimonies point out a number of nuances that go further toward answering the research questions, and suggesting best practice solutions to problems linked to the crime of identity theft. In terms of who are the most common victims of identity, by and large, the greatest proportion of victims would have to be classified as middle class home owning business persons, a few in the financial industry itself. This would make sense, as a target is suitable, according to routine activities theory, according to the value it offers an offender, and it is likely that identity thieves would target persons who would be more likely to have assets that were more exploitable. The fact that in three cases homeownership, moving from one home to another, or retiring and selling a home, were the occasion for identity theft, involving real estate brokers in the reporting process as well, is a point not often covered. Home ownership has always been considered an American dream. This can be a sign of prosperity as seen through the lens of an identity thief... It is likely that as

an industry real estate and the mortgage side of banking would not be protected from, having had little experience with dealing with it, identity theft. Finally, with regard to the business person profile, it is somewhat surprising that in a few cases knowledgeable business persons, including two in the financial industry itself, which is the central focus of identity theft, would have acted in ways that did not seem to be fully aware of the identity theft consequences of their actions. This may indicate just how difficult it is to educate consumers on protective behavior, especially online.

In addition to the most common profile of victim, middle class homeowner business persons, a summary analysis regarding the question of identifying victims must include a comment on the fact that twice children were victimised, and the opportunity provided to thieves by a child's identity is that it is far more likely that they will be able to make use of that identity for years before it is detected, in that children do not engage in commerce using their personal data. It may be that these responses have uncovered an area of great vulnerability in the profile of the identity theft victim. It was similarly found that elderly persons were victimised by identity theft, though once through the agency of a gang-member nephew. Here, too, their lesser level of economic activity, the likelihood that they are unpractised in the ways of finance, or the internet, would seem to offer identity thieves a longer period of time as a window in which to conduct further fraud.

With regard to the question of how long it was before the victim became aware of their victimisation, the answer is split between short term and long term. That is, depending on the mechanism adopted by the identity thief, or the response of a victim to a scam, the victim may have found out about their victimisation soon, but in other cases it was up to three years before they found out. In terms of short-term response, often less than a week, this usually happened if

the crime was based in a physical location, such as a bank, or if the victim had responded to a scam email and, hearing no reply in a day or two, realised that they had been scammed. However, in both cases, the crime had a double time frame: that is, while they discovered that they had been scammed, and often left it at that, lesson learned, they would then subsequently discover that as a result of the scam their personal data had been stolen and used by a fraudster to set up an illegal life, and these crimes they quite often would not hear about for up to three months to a year later. This double-event sequence happened, for example, to #13, for whom it was reasonable to think, after she had discovered theft of her bank account, the problem was solved, but then credit card problems emerged in the months after. When a physical event was not part of the identity theft scam, and when the victim had no idea that they had had their identity stolen, the more common profile is that they heard nothing about it until contacted in one of several ways by stakeholders, at which point it became clear that someone had made use of their personal data to set up a lifestyle. Measured, from the point of view of an offender, then, based on the suitability of target, these findings strongly suggest that it would be in the interest of the fraudster to avoid identity theft based in physical locales, or especially banks, and that even email scams are quickly detected, and suspected, but that impersonal and anonymous ways to steal data are best insofar as they offer the offender a considerable window between crime and detection, in the meantime being able to set up an alternative life. The fact that in one or two cases illegal aliens were able to set up lives for three years, and in another case ten years, indicates how advantageous anonymous theft, defined as when the victim knows nothing about it, is to the offender. In this case, however, the general question asked by victims was, how could this happen? And it is something of a mystery that a thief can make purchases and payments in a false life without his activity ever raising a red flag or being found to be breach. This is clearly a

point, insofar as identity thieves are able to take the time to set up false lives, where security is lax, and detection methodology at present is weak, enabling the expansion of a mere theft into full-out fraud.

(ii) Red Flag and Breach Notification Rules

An additional question was how well red flag and breach notification rules worked, in alerting consumers to suspicious activity on their accounts, or breaches of their account or personal data. The fact up to 15 of 25 victims reported that they had first heard that they had become the victims of identity theft either through a company calling them as a result of a red flag being raised on their account, or from an agency attached to a bank or credit card company who discovered a breach, or even from a credit card company whose red flag and breach notification system was working well, is promising. The research by and large has found that red flag rules and breach notification rules have serious shortcomings mainly because they are reactive and often take too long to get the alert to consumers. It is true that in no case a red flag rule or breach notification happened soon enough to prevent a theft, but they may have cut off an account and prevented future theft. It is likely that as a result of red flag rules and breach notification standard operating procedure mandates changing account or credit card information, in which case this method would cut short the campaign of fraud conducted by means of stolen personal data. It is promising that calls were made by banks, savings and loans, credit agencies, department stores, security companies, and even an auto dealership. This means that more businesses are becoming aware of identity theft and the need to implement red flag and breach notification rules.

It is a bit odder that in some cases either a detective hired by a security company or the police themselves would be the ones to inform a victim of a breach, in one case by police after a criminal had been apprehended with their credit card in their possession. This modus operandi not only seems doubly belated and reactive but two victims pointed out that first contact over this issue involving law enforcement personnel tended to heighten the sense of shame and embarrassment, not to mention shock. This is likely due to the fact that police presence implies criminality, and involving police in the breach notification process may work to cast a pall of suspicion of criminality over the victims. In any case, victims' reports generally present positive news with regard to red flag and breach notification laws that they do work to limit the damage caused by identity theft, and they do seem to lessen the shock of notification. At present, this means of finding out that identity theft was committed against one must be considered best practice.

By contrast, there is another type of call by which victims first heard of their crime against them: calls by credit card companies, credit agencies, department stores, other stores, public utilities, banks, lawyers acting on behalf of clients, and, worst of all, debt collectors, with this type of initial notification occurring in five cases. This represents a serious shortcoming in current anti-identity theft system. The fact that credit card companies honour credit cards with no additional proof of identity, that they take at face value the activity in a credit account, that stores do the same, apparently unaware of the dangers of identity theft, to the extent that persons who do not even have accounts at stores can open up accounts, and they send the bill to them, represents a serious problem. Any call to a victim of identity theft which was undertaken by what we will call a naïve or predatory debt collecting stakeholder represents worst practice in the victims' views. Not only do these calls operate in a world where there apparently is no identity

theft, but they act on the assumption of victim guilt, and generally disbelieve any claim of identity theft as a debtor feint to avoid paying their debt. It is well known that debt collector behaviour can become predatory, advancing into harassment. Victims who first found out about their victimisation in this manner not only found out much later, but experienced the news as much more of a shock. The process to disentangle them from the problem was also much more emotionally taxing, much more time-consuming, and much more reiterative; in the sense that no sooner had they fended off one debt collector, than another began to call. These processes are again no doubt attributable to the dynamics of the debt collection industries, which routinely sells uncollected debt from company to company, for the purpose of eking out a profit from a percentage of payback in even written off debts. It is certainly bad practice for a credit card company or a department store to lack red flag or breach notification rules, or to not be able to discern a real from a fraudulent account; it is unconscionable that credit is able to run up to fantastic amounts, even after no payments have been made into it for years, simply to keep the debt going; it is inexcusable for credit companies or department stores or any business to operate under the fixed assumption that the victim is the one who incurred the debt, and to, in fact, live in a world free of the conception of the existence of identity theft. In the world of debt collection, the name on the card is the guilty party: paperwork is reality, and they operate in that fashion, causing the victim what the research into agency and law enforcement behavior calls revictimisation, when the system, having acknowledged a victim, still treats them in a way that re-victimises the victim, doubling their trauma.

(iii) Amounts of Money Stolen

With regard to the question as to the amount of money stolen in the average act of identity theft, the response of victims presented a surprise. Insofar as the typical profile of an ideal target is a middle class homeowner, perhaps the finding that the amounts stolen usually total into the thousands rather than the hundreds of dollars should come as no surprise. But, generally, with recorded amounts stolen of $70,000 (#2), $75,000 (#3), $30,000 (#11), $45,000 (#13), $22,000 (#18), $12,500 (#21) and with #25 mentioning that all of his assets were gone, it is apparent that identity theft as a crime has dramatically escalated in dollar value amount in recent years (and further escalation will be found in Chapter Six). It is no doubt that these large amounts are the result of gaining personal data to raid bank accounts and run up false credit card accounts: that is, they are a side effect of a simple theft having moved to full-out fraud involving making purchases (with taking out car payments a popular goal) and setting up another life. To the extent that some illegal aliens used stolen personal data to collect social security or to purchase a house, the amounts are much higher. The higher amount mentioned was $2 million, at which point the global, organised labour scale of the crime is clear. Again, it is disturbing that credit card accounts allow for these excessive withdrawals or expenses without any kind of red flag, should they diverge from the record of purchases by the person whose name is on the card, and have no safeguards to limit the total damage. In sum, however, the respondent victims in this study indicated that not only is the average dollar amount total of their victimisation large, but that the crime has morphed to take most advantage of credit account fraud and setting up a fraudulent lifestyle. Insofar as the research generally found that this motive was not high on the list of offender motives, victim reports contradict that finding.

(iv) Resolving Problems

With regard to the question of how long it took to clear up the problem, here too, there seems to be a double-sided answer. In terms of the immediately detected crime, and protecting oneself from any further damage being committed on, for example, a stolen car, changing PIN numbers, or card numbers, or even closing accounts, would seem to stop the crime in fairly short order. But for middle class home owning consumers in particular there is the larger issue of protecting their credit score in order to enable them to make purchases, without high interest rates, and purchase major consumables, including houses. In this regard, in the larger, more emotional quest to clear their name, the reports indicate that it takes years. The figures provided indicate one year (#1), 13 months (#2), a year and more (#5), six and a half years (#6), seven years (#7), almost seven years (#13) one and a half years (#16) sixteen months (#17) and ten years (#25). Others, report even longer consequences, with the word ongoing (#7, #11, #13, #14, #15, #21, #23) frequently recurring. #11 described even an ongoing process as moving at a snail's pace, and #23 fatalistically believed that he will be dealing with it for the rest of his life.

The exception to these are persons whose crime was quickly detected by an organisation that protected them, with #21 being offended and miffed that it would take a bank two weeks to reimburse her, but, comparatively speaking, this ended the problem for her, and #10 complaining over two weeks and a few work days lost, but clearly his company, where he was a senior VP, had a solid support structure and resolved the problem in short order, with no further consequences. These responses again appear to suggest that if the crime happens under the aegis of an organisation that has in place a solid structure of red flag, breach notification, reimbursement and preventive and corrective action policy, the time taken to resolve the issue is much less, and much less traumatic for the victim. It is therefore a good thing for a person to discover identity theft through a bank account, for example; similar advantages accrue from

being involved in a massive scam that affected other users of on online service. When, however, a person has no idea how the information was stolen, and finds out about it after the fact, after the fraudster has been able to build up a false record, and no particular organisation or agency takes responsibility for the crime, then there is a serious mess that usually forces the victim to bring a lawyer in to resolve it. Once again, debt collection agencies, linked to credit cards companies or not, who make calls strictly to collect debts, and for no other purpose, and especially when, after an increasingly short time, a legitimate company passes on a bad debt to a debt collection agency, the involvement of this kind of stakeholder at this point can greatly complicate and retard the recovery process, at the same time adding so much to the trauma of the event that the victim is clearly revictimised, and will begin to lose faith in the whole system. It is clear from these victim responses that the current means available to help victims recover from identity theft are inadequate, and directly contribute to the fact that the crime is traumatic for so many victims. The fact that the length of the process, the inability to resolve it, most often causes the victim to characterise this crime as a "nightmare" speaks for itself.

(v) The Involvement of Law Enforcement

By far the worst form of enmeshment in the labyrinth of identity theft, and the entry point which is experienced most often as a nightmare, and with the most offence by the victim, is when law enforcement becomes involved in responding to the report of the crime through indirect means. #5 went to the DMV to renew a license and the helpful person at the DMV believed the paperwork not the human being and called the police, causing #5 to spend a night in jail, surreality suspected of being the identity thief of his own stolen identity. When #6 applied for his first telephone, the salesperson found that a phone already existed under his name, believed the paperwork over the human being, called the police, who responded in person, became

difficult when there was resistance, and the victim ended up being the only person almost arrested in this particular crime. The most outrageous example of a police record-keeping database-based system of surveillance clashing with the world of identity theft was when #9 was stopped on the road, his license plate number flagged in a database, and taken off to jail because the person who had stolen his identity subsequently committed murder in South Carolina! When #1 was called down to a police station and #22 was lead to a police station to file a complaint, even these incidents seemed to arouse in victims a feeling of victimisation. This kind of police involvement in identity theft detection would appear to be far below best practice, given the re-victimising outcome of their participation.

Indeed, in response to a question about other negative outcomes, victim responses reveal that identity theft is a highly traumatic crime. #5 reported that his wife was hospitalised due to the stress involved, #15 reported being depressed and having to see a psychiatrist, #17 reported feeling like he was going out of his mind, #18 felt anger, frustration and shame, #22 reported that when told of the crime her whole world stopped, #25 lost her husband due to his suspicions of her, and her home; in short, though forensic studies would have to be undertaken to compare the traumatic outcome of experience of identity theft to other crimes, this is strong anecdotal evidence that identity theft leaves a permanent mark on a person's life. This can also involve their trust in the system, in law enforcement and in law makers, and may likely turn them against illegal aliens and immigrants as well.

The question has to be asked, were they in any way, according to routine activities theory, to blame for their victimisation? That is, did they expose themselves to identity theft by engaging in any off- or online behavior that could have been avoided? The answer to this is yes and no, that is, some victims did stupid things, which contributed to their identity theft, others

could not have foreseen the theft. #1 left behind a lock-box in an office destroyed on 9/11, #3 had her data stolen by her nephew who was a gang member, #4 was indirectly victimised when a data broker was hacked, #19, #20 and #24 were victimised by rings of illegal aliens in ways that appear to run circles around their capacity to protect themselves and #22 suffered at the hands of lax forwarding of mail by the USPS and a criminal newcomer to their old address. While the organised crime dimension of the crime has been detected in the offender part of this study, from the victim's point of view it seems difficult to protect against it. The other incidents could be classified as unpredictable, and hard to defend against, but represent opportunism or every day criminality beyond the scope of most average citizens to comprehend (it would be interesting to reconstruct how in fact #1 data got from its lock-box on 9/11 into the hands of an identity thief). On the other hand, #10 and #11 responded to a phishing effort, a classic scam, while #15, overeager to find work via the Internet, made a classic error of providing data and fee before verifying services received. Even #18, whose home was burglarised, could have made his target a bit less suitable for offenders. At present, however, that represents only one fifth of victims reported on having acted in ways that a training or consumer awareness program under routine activities theory protocol would protect. By and large, the impression is given of offenders finding ever newer ways to steal identities, consumers as vulnerable potential victims, and identity theft as a criminal opportunity continuing to spread virally into every part of everyday life.

Finally, there is the issue of law enforcement response, the guardianship aspect of a routine activities theory framework for identity theft. Mention has already been made of two means by which police have entered into the identity fraud from the point of the victim: if they or detectives connected with a crime become part of the mechanism that notifies the victim of a

breach, their involvement found to be somewhat traumatising by victims; or if they are conducting business as usual in detecting criminals, false data comes up on a database, and they stop or detain victims under suspicion of being the person who stole their identity, a circumstance which is always traumatising to the victim and always re-victimising. It is arguable that policy should find ways to remove police from involvement in identity theft in either of these ways. It is also arguable that the only way that the police should be involved in fighting identity theft, in terms of coming in contact with the victim, is when the victim deems it necessary to file a police report of the crime, which has complications, and if their case of theft becomes part of a larger case, in which case police participation might be helpful. But it is not clear that police know how to proceed in cases of identity theft. #1 was asked to come down to a police station to "straighten out a confidential manner," it is likely that the officer remained vague in order to adhere to policy, but this request was interpreted by #1 as adding insult to injury, and felt like a victim suspected of something. When #3 came in contact with local police, the fact that they were not sympathetic and "acted like this crime is out of control" resulted in him "never feeling more violated" no doubt because he expected a measure of validation from the police. #7, #17, #20, #22 and #25 all, having come in contact with the police, were under-impressed by their response, as it was apparent to them that the police did not know what to do, and, in fact, one police officer informed victim #11 that, explicitly, there was nothing they could do because in his case the crime was technically committed overseas, out of their jurisdiction. #25 even contacted the FBI first, who told him to contact his local law enforcement agency, which then "did very little to help and investigate" leaving him feel not only like law enforcement had given him the run around but that no one could do anything for him. #23 was told to contact the Federal Trade Commission as well as the police, indicating that different

stakeholders were telling him different things he had to do, meaning that there is no single system in place. In #12's case, an investigation was actually launched, but it was moving at a snail's pace and had become frustrating (but #12 still did seem to have faith in the police). #15 went to the Attorney General, or rather, the case was such that the Attorney General saw fit to look into it, and those who got no satisfaction from the police evoked politicians and laws as the ultimate solution to stopping the viral spread of identity theft. #23 had frustrated recourse to the title of an old newspaper cartoon, there autta' be a law, while #24 pleaded that a politician is needed, that somebody needs to do something.

Therefore, in response to the question, what did the police do, and how did the victim respond to or perceive police action, it is clear that most victims were uniformly under-impressed by law enforcement response, quickly caught on that law enforcement has no response, were even told that there was nothing to be done, and generally were given a run around or subjected to slow investigations by those who did not want to admit such a thing. The failure of guardianship espoused by offenders as the number one reason why they continue to or have migrated into commission of identity theft is therefore further confirmed by these findings, at the other end of the equation. Even a population of victims unversed in the procedures of policing can recognise a law enforcement paradigm that is unresponsive and helpless before identity theft. Finally, there is also little question that the failure of the police response, its inappropriate involvement in other stages of the reporting of the crime, greatly contributed to the stress resulting from the crime. The fact that victims felt out of control, and that there was nothing they could do, made the processing of the crime much worse than the crime itself. While negligence and not being able to do anything would not constitute another example of police revictimisation,

it certainly contributes to the overall sense of desperation that clouded just about every victim response to the research questions.

With regard to the validity of victim responses, it was noted that the highly emotional nature of their response tended to focus them on one signal aspect of their experience, often resulting in them overlooking other points. Most victims seemed uninterested in detailing the specifics of what steps they took after the crime, such as closing an account, to protect themselves. By far, the main theme was the shock of the crime, likely due to their unfamiliarity with it, and the complete inadequacy of response. From the victim's point of view, identity theft at present, from the perspective of law enforcement, is like a few other crimes, possibly traumatic, and subject to revictimisation by the system. Both of these elements must be stripped away from procedures in a new best practice that provides consumers with a sense that their problem will be addressed, the offender will be caught, and they will not be revictimised by the debt collection, breach notification or law enforcement systems.

(d) Conclusion

The results found that the primary target for identity theft are middle-class business persons, often home-owners, whose assets would represent an attractive target, though children and the elderly are also deemed suitable targets to the extent that it may take some time before the theft of their identity and the creation of a fraudulent life based on it is discovered, as their use of credit cards and other instruments is not frequent. By and large, victims found out in the short-term, if the crime was committed against a physical carrier of identity, at a bank, or as part of an Internet phishing scam, but, then, that it took much longer for a victim to become aware of

the further consequences of theft, that is, later use of credit cards and accounts for purchase of goods and other assets. In the former case, discovery was made within a few days or weeks, in the latter it could take up to three years. Contrary to research which disparages them, red flag rule and breach notification law-based alerting of consumer of suspicious activity on accounts remains the most effective firewall against identity theft becoming worse than it is. By contrast, for the victim to hear about the crime through a credit card agency, a department store or a debt collector, all determined to collect debts on the stolen card or account's name, is far less optimal, and police involvement in this process is particular damaging. The amount of assets stolen through identity theft is larger than perceived generally in the research, with middle class business persons routinely reporting losses in the tens and in some cases hundreds of thousands of dollars, these large totals reflective of the drive by more organised theft rings to exploit stolen identity to build up false identities and pillage accounts.

Generally, specific problems related to identity theft, like compromised credit cards and checking accounts, can be cleared up in a matter of weeks, but the effort to clear up one's credit record and to stop credit card companies or debt collectors from continuing to contact one for collection purposes can take up to seven years to a decade. If a stolen identity and its records become enmeshed in a police department information system and are taken at face value then the consequences can be particularly problematic for the victim. As a result of the secondary victimisation of victims of identity theft by the debt collector aspect of the notification system as well as the difficulty involved in clearing their credit name, complicated if they had little knowledge of identity theft in advance, identity theft can be classified as a traumatic crime resulting in numerous negative psychological impacts and long-term negative impact on the lives of its victims. While in some cases, especially involving phishing, it is possible that routine

activities theory-motivated training or consumer awareness could prevent some ill-advised behavior by consumers, it is also true that several victims became enmeshed in theft through unforeseeable pathways that only testify to the fact that identity theft is slowly spreading virally through all aspects of electronic-based commercial life. Finally, victims were overwhelmingly under impressed with both the manner in which law enforcement was involved in identity theft, the pace of their actions against identity theft, and generally appalled at the apparent and some espoused helplessness of the police in doing anything about this kind of crime. This lack of guardianship was perceived by victims as one of the leading causes of the crime and certainly was cause for them to be even more traumatised by the apparent out-of-control, nothing-can-be-done nature of the crime. On the basis of these findings, with regard to victims, it is recommended that all consumers with bank accounts over a certain amount and who are home-owners or owners of assets as well be offered identity theft awareness literature or information as part of their routine activity, that red flag rules and breach notification rules be strengthened, and enforced more vigorously in all industries that make use of consumer personal data (with department stores in particular appearing to act innocent of the problem), that the debt collection industry be mandated to check with credit card companies and banks the authenticity of the identity data that they have been given before they contact consumers, that red flag rules and breach notification awareness be inculcated in that exploitative industry, that the dollar amount of identity theft be limited by additional restrictions on open line of credit use, that police be excluded entirely from the breach notification side of victim contact, that all data in police databases be checked against identity theft databases to prevent untoward police action taken on the basis of stolen identities, that police awareness of identity theft with regard to its potential in all industries and scenarios be broadened, and that an intermestic framework be developed which

encourages tarns-jurisdictional response to identity theft so that police in one jurisdiction are not left to tell victims that there is nothing that they can do. In all these ways, through removing several aspects of offender motivation, consumer awareness, strengthening, expansion and reorganisation of the red flag and breach notification system, and shoring up and improvement of law enforcement involvement in the process, it is hoped that the crime of identity theft, now experienced by victims as a traumatizing event of almost existential proportions, can be greatly alleviated.

Chapter 5: Offender Motivation and Organization

(a) Introduction

Chapter 5 presents the findings of research question three, with sub-questions: who are the identity thieves, what means do they use to commit identity theft and how did they acquire the skills that are needed to commit identity theft? The findings expand upon current research by determining that identity theft opportunity arises in a much more complex way than currently conceptualized, and that identity thieves are coming into the crime from a myriad of different pathways, previously unsuspected. The findings, therefore, indicate that current definitions of identity theft, from the offender's perspective, are limited in terms of how offenders enter into identity theft crime, the methods they make use of to commit the crimes, and their perceptions of why they continue and will continue to commit identity theft.

The chapter is exploratory and is designed to consider offender motivation and reveal his/her perspective. Interviews were conducted with some individuals who had been incarcerated and others who were not in custody, pre-and post-convictions for identity theft crimes. The interviews were an in depth analysis of the social causes, the attitudes towards the public, ignorance, and the effect caused by governmental inaction. Actual cases were delineated in conjunction with the personal interviews. The interviews also illustrated the organizational aspects of identity theft schemes. Identity theft related crimes require entrepreneurial skills, an ability to gain access to the information of others, the personality of a con artist, as well as, social and computer skills. This chapter further shows that not all offenders have the same goals. Some offenders have the desire to amass wealth, succeed and live a respectable, comfortable life

within society while hiding their theft; others operate with less caution by taking chances as opportunity arises.

To reach a conclusion about each offender's motivation and organisation of identity theft, the interviewer examined the following: social status, education, ethnicity, religious beliefs, age, prior criminal activity as well as, arrest record, current family status, financial ambition and the non-confrontational methodology of this particular crime. Notably, there is the possibility that these subjects may not have been forthright during their interviews; they may have downplayed their culpability and rationalised their own behaviour in fear that their words would be used against them.

(i) The Current State of Awareness

Before presenting the data obtained in this study, a brief review of pre-existing findings in the research, along with a brief review of the methodological frameworks as presented in Chapter Three, is presented, for the purposes of comparison.

Statistics

Identity theft is commonly perceived to be a white collar crime rather than a vehicle for the low level, street criminal; however, individuals who commit identity theft do not fit into any specific financial class. Some of those individuals are relatively intelligent individuals, although their academic achievements are not necessarily their strongest asset. Copes and Vieraitis (2009) discovered that identity thieves were from various occupations. They also stipulated that identity theft may not necessarily be classified as a white-collar crime, committed by white-collar offenders.

Additional figures passed on by (FTC 2012) showed that for calendar years 2007 through 2010, the 20-29 age groups experienced the highest rate of identity theft of seven age groups that were surveyed. A 24% rate was experienced for the previous five years (FTC 2008, 2009 2019, 2011). The 30 -39 age groups fared slightly better for the same period, reflecting from 21-23% for the same years (BJS 2011).

A recent Crime Data Brief written by Langton (2011) showed an increase in identity theft victimisation from 2005-2010. The Bureau of Justice statistics (2011) showed a 50% increase in the misuse of existing credit card accounts per household from 2005-2010 from 2.5% to 3.8%. However, the data reflected a decrease in the misuse of personal information when used to open new accounts; there was a 30% decrease from 2005-2010 from .09% to .06%. After a comparison of 2005 and 2010 statistics, figures also showed the lowest victimisation rate by age is for those 65 and older. When comparing figures for a younger age group, 12-17 years, there was a 10.2% increase amongst victims.

A non-Hispanic white comparison for years 2005 to 2010 showed a 7.3% increase in identity theft victimisation in 2010 when compared to a 5.8% in 2005. However, there were similarities of same numbers among non-Hispanic black and Indian-headed households and non-Hispanic persons of two or more races.

There was a household increase in identity theft from 2005 to 2010 regardless of the marital status. A comparison showed a married head of household experienced a 5.9% in 2005 and an 8.0% in 2010. Households with a non-married head experienced a 5.1% in 2005 and an 8.0% in 2010. The 2005 to 2010 household income of $75,000 and above showed a 9.5% and a 12.3% increase in identity theft respectively. There was a slight identity theft increase within

households with less than $7,500 from 2005-2010 of 4.7% and 5.3%. There was no change in the lesser known income households.

Copes and Vieraitis (2009) have shown that a large number of identity thieves were between the ages of 25 and 44 years old. In 2007, Rebovich (2007) conducted an empirical, identity theft study with permission from the United States Secret Service. Closed cases 2000 – 2006 of 933 offenders were analysed for offenders' characteristics. The age group that reflected the most offenders were between the ages of 25 and 34 years of age (347) and reflected 42.5%. Offenders reflecting 35-49 years of age (270) were 33% of the study group. The 18 to 24 years (151) group comprised of 18.5% the fifty years and older (49) made up 6% of the study (Rebovich 2007:31). Copes and Vieraitis (2009) postulated that the largest number of offenders were from the White population. However, Rebovich's study showed that offenders within the black population were in the majority with 53.8% (467) out of 922 defendants as reflected in their arrest histories. Of the 922 offenders files that were looked at, 38.3% were White offenders (332). The Hispanic population showed 4.8% (42) and 3.1% were Asians (Rebovich 2007:32). This researcher found that identity thieves represent a variety of age groups.

The below listed table (table) summarizes 25 offenders (who were interviewed for this research project) background/history.

Offenders Background/History

Table 8

OFFENDERS	STATE/COUNTRY	M/F	AGE	RACE	STATUS	OCCUPATION	OFFENSE	EDUCATION	SENTENCING
A	New York	M	33	W	M	Truck Driver	ID theft	H.S	State Prison
B	Pasadena CA	M	49	W	M	----------	ID Theft	College	State Prison

OFFENDERS	STATE/COUNTRY	M/F	AGE	RACE	STATUS	OCCUPATION	OFFENSE	EDUCATION	SENTENCING
C	New York	M	32	B	M	----------	ID Theft	H.S	State Prison
D	Jamaica	M	30	B	S	Clerk	ID Theft	H.S	State Prison
E	New York	M	42	B	D	Laborer	ID Theft	College	Prison
F	Mexico	M	22	W	S	Laborer	ID Theft	H.S	Deportation
G	Yugoslavia	F	21	W	M	Student	ID Theft	College	Prison
H	Moldova	F	26	W	S	Student	ID Theft	----------	Prison
I	Moldova	F	31	W	M	Hotel Recep.	ID Theft	----------	Prison
J	Moldova	M	31	W	M	Jeweler	ID Theft	College	Prison
K	Russia	F	35	W	D	Au Pair	ID Theft	----------	Prison
L	Moldova	M	40	W	M	Mechanic	ID Theft	H.S.	Prison
M	New York	F	25	B	S	Clerical	ID Theft	H.S.	Prison
N	Dom. Rep.	M	24	H	S	Waiter	ID Theft	H.S.	Discharge
O	S. Carolina	F	20	B	S	Clerical	Theft	H.S.	Spilt/Sent.
P	Virginia	M	33	B	M	Construction	Theft	--------	Prison
Q	----------	F	29	B	M	Accountant	Theft	College	Probation
R	Ramallah	F	38	A	M	----------	Theft	----------	Fines
S	Russia	M	38	W	S	----------	Theft	----------	Prison
T	New York	F	54	H	D	Hotel Maid	ID Theft	H.S.	Probation
U	Haiti	M	60	B	M	Limo Driver	ID Theft	H.S.	Split/Sent.
V	New Jersey	M	27	W	S	Real Estate	ID Theft	College	Plea Bargain
W	New York	F	25	B	S	Travel Agent	ID Theft	College	Prison
X	New York	M	49	H	S	Cust. Service	ID Theft	H.S.	Split/Sent.
Y	New York	F	50	H	M	Sales Rep.	ID Theft	College	Prison

(ii) The Data

In this section, descriptive reports of encounters with individual identity thieves are reviewed. First person usage is retained, in the interview sections only, to highlight the personal

nature of contact with these individuals in the field, as part of my professional life, in an ethnographic context. As such, then, the "I" is an index of the various opportunities and constraints on contact, reliability, reluctance, means of gaining data and means of reporting data that circumscribed the interview process.

(b) Individual Cases

Though 25 interviews were undertaken with offenders, a select few stood out for the insight offered on offender motivation and methods, and are treated here.

Jake (all names are anonymized)

The identity theft market is influenced by supply and demand. An explanation as to how the market functions is necessary. First there are the thieves, the purchasers, the distributors and the receivers. Even though there are regulatory policies in place to prevent illicit activity in the identity theft market, the thieves continue to ply their trade with little or no fear. During my tenure at the Manhattan District Attorney's Office I had the opportunity to interview Jake, an identity thief, during the course of an open investigation. After the official interview was concluded, I offered Jake a cup of coffee and a bagel from the kitchen in the Detective Squad. I explained to him that I wanted to have an "off the record" dialogue about how he committed his crimes. I further explained to Jake that he should forget about his past crimes, of which, I considered those transgressions to be "water under the bridge" because he had previously answered for those crimes. I informed Jake that I was looking for a blueprint to understand identity theft and that my informant had told me that he (Jake) could provide me with the information that I needed. Jake asked for six packets of sugar to sweeten his coffee and after it was consumed along with the bagel, he told me that when he went out to "see about his

business," he would occasionally frequent bars and night clubs on the Lower East Side in New York City in order to "make some money.

JN: *Did you have an opportunity or an objective to "make money?"* Jake: Yeah, I sweet talked and picked up broads who had a little too much to drink, followed them back to their place and got laid. As soon as the broads fell asleep, I went through their handbags, their mail and took whatever I could find with their personal identifying information. Some nights I worked over two or three different broads in order to steal their stuff. *So you weren't afraid doing this?* In the beginning I was jittery but then I felt more comfortable. *Why?* Cos the more information I stole, the more money I made and don't nobody get sent up the river for doing this when you are too good at it. You see Detective Judy; I had to report to a recruiter working as a middle man for the dude at the top. My recruiter said that the man at the top was looking for social security numbers, birth certificates, credit cards and official looking mail. He gave me $50 for each piece of good Id's they could use. *Do you know what happens to the stolen info after you hand it to your recruiter?* Afterwards I found out that all of that information was mass-produced into good Id's. The Id's were then sold over the net to illegal immigrants from Russia, Mexico and the Caribbean. In order to substantiate Jake's accounting of the previous answer, the next question was asked: *Did the recruiter say that the good Id's were sold to illegal aliens?* No Miss Judy, the DA read it out in court and my lawyer showed me a copy of the affidavit that was written against me when they brought me up from the pens for arraignment before the Judge. (Jake)

Jake then became restless, expressed his desire to leave, and explained that someone was waiting for him uptown. I gave him my business card and told him that if he wanted to "talk" further that he should give me a call. Jake asked to use the men's room and later rushed out the door. The interview lasted approximately 44 minutes. I was not given permission to take notes;

therefore, I rushed to my desk, grabbed a notepad and recapitulated whatever I could remember in detail. I realized that time was of the essence while the interview was still fresh in my mind.

Joe

The opportunity to interview Joe, who "worked" for a New York-based organised crime family, occurred when my work partner Don and I were accompanying him from Los Angeles, California, to New York City, on a felony, court-ordered extradition warrant. Joe divided his crime ventures between Los Angeles and New York. He was finally caught by the Los Angeles Sheriff's Department for running a red light on Wiltshire Boulevard while driving his 1960s Mustang. A warrant check was conducted against Joe's name, which showed that he was wanted in New York City for identity theft. Joe, whose arrest record showed time served for committing commercial and residential burglaries, chose to offend as an identity thief because the sentences were not as severe or risky as committing burglaries. Joe was happy to get a free escort back to New York City so that he would be incarcerated on the east coast; he could be close to his wife and kids and also receive conjugal visits. As we settled on the plane, I asked Joe if he could provide me with his roadmap to stealing identities. He obliged.

Joe: "I started working for one of the families (the syndicate) ... went to jail a couple of times for not doing my thing with common sense. It was in jail that I changed my life around for the good of my wife and kids. I met somebody in the can who introduced me to stealing identities ... decided to get involved in stealing identities after I realized that I could make money using people's information such as name, address, Social Security number, driver's license number, mother's maiden name, and date of birth. JN: *Did you calculate the risks involved with fooling around with other people's identities?* Yes. But at the time I also learned that a mother's maiden name was the best piece of information you could get to apply for a birth certificate

because you could do a lot of things like ... apply for any help to get welfare and food stamps ... make up Ids to trade or sell or use it for yourself so that when the DTs (Detectives) catch you... they think you're clean."

After taking a quiet moment, Joe further spoke about the documents that he acquired from stealing people's information.

Joe: "Me and my friend surfed the Internet for websites, which buy personal information. I scanned all the information with the Social Security numbers, dates of births, driver's license numbers and whatever I could find. I sent about 10 to 12 sheets of information to the Internet (website) addresses twice per week and they sent me $600 per batch of stolen stuff through Western Union. From the very beginning, I learned that the risk of getting caught and doing time is very low, but the profit is good. Me and my boys know that most of the times the cops take a long time to catch up to us and it is even longer when people live far away from each other so they don't want to be bothered travelling to testify against you. This is just easy to do with lots of opportunities to make good money. Most of the times the Judge will give you probation or community service, even if the DA ask for jail time for you. *Do you fear serving time in prison?* Not really...if me and my boys have to go to Rikers (jail) for a little while ... we can get good practice when we are in cause ... there is a market for everything you trade in the can."

The threat of incarceration does not discourage persistent offenders like Joe and his crew because identity thieves can still function from behind prison walls. Joe's crew consists of gang members who continued to run their outfit (operation) whether they are roaming the streets freely or incarcerated in the local, state or federal system. They are also aware that identity theft crimes are difficult, expensive and time-consuming for the authorities to investigate, especially when multiple jurisdictions are involved. Thieves take advantage of this knowledge by stealing

identities in one state, using the same identities in other states and eventually, trading or selling those identities for use in foreign lands such as Lagos, Nigeria, Cape Town South Africa, throughout central and Latin America, Asia and also in Eastern Europe.

Bobby

During an assignment to transport an inmate to New York State Supreme Court, I had another opportunity to interview a convicted identity thief. The inmate was incarcerated at the Metropolitan Correctional Centre in Lower Manhattan on an identity theft and conspiracy charge. The federal jail is located approximately two blocks from the Manhattan District Attorney's Office. The inmate/witness Bobby was scheduled to testify against a defendant in Supreme Court on a robbery case. When my partner, Mark and I arrived in court with Bobby, we were immediately asked to return him back across the street to the federal jail because the defendant had just accepted a plea bargain from the prosecutor; as a result, Bobby's testimony was no longer necessary. I explained to Bobby that we would return him to the "Feds" right away. Bobby informed my partner and me that his blood sugar was low and he needed something to eat. I bought Bobby a grilled cheese sandwich and a can of Pepsi from the coffee shop, which is located on the first floor of the Manhattan Criminal Court building at 100 Centre Street.

We sat in an unoccupied corner of the coffee shop for privacy because Bobby was restrained by shackles and handcuffs. Bobby thanked me for my kindness. It was at that point that I told Bobby that I was a research student and I needed information regarding how identity thefts were committed. Bobby looked surprised and wanted to know why I thought he knew about identity theft. At that moment, I pulled out a copy of his criminal record (rap sheet) with

his photo and said, “Come on Bobby; I have the goods on you. I know what you do for a living.” Bobby unexpectedly agreed to be interviewed for this study.

JN: *So, why did you choose ID theft?* Bobby: I am not a real ID thief. I only got into this because it was part of the ceremony for my gang initiation. We had to prove that we could steal Ids from people. If you were good at it, they would initiate you pronto and it became your speciality as part of your job. We broke into apartments, houses and cars so that we could take whatever information about a person we could find. *Why did you choose those methods?* Cause they were all easy to do. We worked four at a time and had to have a girl with us... they distract other people and can pretend that they always need help with anything... they don’t get too nervous and they keep their voices the same tone. We hit (burglarized) houses late in the morning hours after rush hour because most people go to work and kids go to school. *Weren’t you afraid of being caught?* No. Cause we pretended to be landscapers or delivery people. We drove around the neighbourhood and watched for people to leave their houses... then we went in through a back window or door and then we would let everybody in. We took information on credit cards, safes, family photos, mobile phones, birth certificates and utility bills ... sometimes; we would even take whole drawers of paperwork. After we brought back the looted information to the person who was responsible for processing out what was needed to start making Ids, then other people hacked into websites on the net to get credit bureau reports. *On the victims?* Uh huh.... once we got that information, other kinds of bogus Id’s were made up. *Such as?* Credit cards, car loans and then we applied for duplicate Social Security Numbers. Some gang members were trained to be shoppers. There were the ones who bust out the credit cards at big stores like Bloomingdales, Macy’s, Saks Fifth Avenue and Apple. They bought all kinds designer merchandise like, Lalique´ perfume, Louis Vuitton bags, belts, shoes, watches and jewelry. They

shopped for cars that were immediately shipped to countries in Eastern Europe, parts of the Caribbean and Central and Latin America.

Michael

In October 2008, my working partner Walter and I were assigned to extradite an inmate from York, Pennsylvania, to New York City, to answer charges for identity theft. We travelled by automobile. After securing Michael, the inmate, in our car, I realized that our journey back to New York City would take a couple of hours because of the long distance that we had to cover. At one point, we even made a stop at a rest station for about 15 minutes so that everyone could stretch their legs. I asked Michael about the status of his education, family and friends. After we arrived back in New York and my official duties were complete, I showed Michael my expired identification card from John Jay College and asked if he was willing to talk to me about some methods he used in stealing identities. He agreed. While preparing for Michael's extradition, I realised that he had been in the business of stealing identities for two decades.

JN: *What makes you tick? Tell me about yourself.* Michael: When I was 17, I started out as a lush worker and rode the subways in New York from the beginning of the line to the end searching for people who were drunk. I always had a razor for protection ... so I cut their pockets ... some ... I just turned their pockets inside and out, took their wallets or pocketbooks, emptied everything inside my knap-sack and split. Sometimes I would go down to the Union Square Station at rush hour ... and learn to pick the passengers pockets ... Cos the train used to be packed ... business was good for me. Sometimes, if I got caught, I pretended that I couldn't speak and they (the police) would let me go. One day I rode the trains all night and couldn't make any money because the new class of rookie cops was riding the trains. They cramped my

style. I needed money and so the following day, I sold as much information as I could to another thief who took me to an address in located in a basement, the Bronx and they made a driver's license and two credit cards for me ... They hit me up for $25 for the IDs. I used one of the credit cards to rent a room in a single room occupancy hotel for me and my girlfriend for about two weeks before we moved on to another hotel. About eighteen months later, my luck ran out on me ... a group of decoy cops who were doing a sting operation against lush workers finally caught up to me... I was locked up and the Judge sentenced me to one and a half to three years ... No I am facing deportation back to Jamaica. *Why are you facing deportation?* Cos ... Me nah citizen ... Me from Jamaica man.

Harold

My informant, Charlie Hustle, introduced me to five of his old friends, who are also ex-offenders, with the expectation that they would participate in my study. Only one individual by the name of Harold expressed an interest in my research. Harold said he needed $135 in order to pay his cell phone bill that would soon be disconnected. After realising the importance of this study, I agreed to pay Harold's phone bill, hoping that an interview was imminent. We stopped at a Chase bank on Canal and Mott Streets in Manhattan, and I withdrew $135 to prevent his cell phone service from being interrupted. Harold was very pleased after receiving the money and commented after my first question was asked:

JN: *Now... let's talk Harold... what do you know about Id's and the way people go about stealing them?* "Me and my friends go through dumpsters outside of hotels to collect cans so that we can take them in for money. One day I found a letter with a credit card in the dumpster. I didn't know what to do. I looked for my friend and showed him the letter and the card. He was

undecided about what action he should've taken with the information that he held. We went to a store on the west side of 42nd Street ... gave the credit card and the letter to the guy behind the glass partition ... paid $55 and walked out with a another credit card in my pocket." (Harold)

Even though Harold swore that he did not intend to go into the identity theft business, his journey continued. He further explained,

"I started stealing cell phone bills from unlocked mail boxes. Then I would reroute mail to my friend's addresses by filling a change of address card at the post office... then I made a lot more new identities. We sold the IDs to illegal aliens and to people who like to shop. The shoppers sold their things to bodega owners in Washington Heights, Manhattan."

Fatima

On August 20, 2008, Fatima Monahan plead guilty to stealing over $45,000 from her former employer, the founder and managing partner at a private equity investment firm located on Park Avenue in New York City. Monahan worked as a personal assistant from August 2005 until November 2006, when she was fired. Monahan's responsibilities included scheduling appointments, booking flights, making hotel reservations, opening and sorting mail, and other administrative tasks, which included preparing checks for the payment of personal bills. Court transcripts revealed that from June 2006 until November 2006, Monahan used her boss's American Express credit card for personal expenses via the Internet for the majority of her purchases. She bought high-end clothing, shoes, children's wear, food and household items, ranging from kitchen utensils to sheet sets from various online stores. Monahan also purchased and used gift cards from Bergdorf Goodman. Monahan plead guilty to Grand Larceny in the

Third Degree in New York State Supreme Court. Under the terms of the plea, the defendant was ordered to pay $45,000 in restitution and was sentenced to five years probation.

(i) Dave (hotel employee)

In December 2009, while searching the apartment of an identity fraud suspect, detectives from the Manhattan South Grand Larceny Task Force discovered financial records, which belonged to75 former guests of an exclusive New York hotel. The offender, who will be called Dave, had been dumpster diving and found personal documents that were discarded into a trash bin near the hotel. An investigation was conducted after an alert hotel employee witnessed Dave reading and collecting pieces of paper from the trash which was discarded by employees at the hotel. Surveillance cameras were set up at the location whereby Dave was eventually arrested; unfortunately, Dave had already created false documents, including driver's licenses, photo identifications, social security cards and birth certificates by using names of some hotel workers. In addition, some of the documents were used to purchase clothes and electronics which were sold to a fencing operation. It was later revealed that one of the victims was alerted to the scam by a credit agency. The agency had flagged the victim's name for a notification and informed him that someone had used his identity in order to obtain credit cards and applied for a mortgage. Dave's criminal actions resulted in a high degree of exploitation for the sake of a lifestyle which included identity theft. Dave pleaded guilty to identity theft and was sentenced to one year in jail.

(ii) Brooklyn Offenders

I also interviewed four fraudsters who committed their crimes alone. Two of those men worked in gas stations in Brooklyn and the other two worked in retail stores. The majority of cases that I examined, in addition to court hearings that I attended, indicated that these crooks worked alone. Some concepts of the crimes that were analysed did not fit into the identity theft

mould. They all admitted that for various reasons they committed their crimes alone. One of them worked in a gas station, the second one worked in a large retail store, the third one was unemployed and had others doing "the business for him" and the fourth person was a burglar. Some of their crimes were organized; however, these four individuals did not believe they fell into the typical identity theft equation.

In addition to accessing the above information, documents that were found in court records were examined. Additional information was elicited from defendants after their cases were called and sentences were negotiated with the prosecutors, Judges and Probation Officers. It is not uncommon for convicted felons to reveal further details about their crimes after sentences were imposed; many defendants were willing to speak candidly about their offenses. At the end of one interview session the defendants exclaimed, "We made out real big because we had nothing to lose, the sentence was a joke." Most defendants were willing to take risks at re-offending and were not concerned with the penalties that are in place against identity theft. The offenders stressed that they surreptitiously operated alone. In doing so, they felt that their chances of being arrested would be slim to none. In addition, they felt immune from prosecution because their cases would be dismissed or worse case scenario, they would even receive a "slap on the wrist" for the perpetrated crimes.

(iii) Summary Analysis of Individual Testimonies

On the basis of the interviews, a general model of the modus operandi of these identity thieves can be sketched out. First, the identity thief attempts to acquire a victim's personal information. Criminals must gather personal information, either through low-tech methods such as stealing mail, pilfering workplace records, or dumpster diving or through complex and high-tech methods, such as hacking into someone else's computer or by the use of nefarious computer

codes. The loss or theft of personal information by itself, however, does not immediately lead to identity theft. In some cases, thieves who steal personal items, such as computers, wallets, phones, etc. inadvertently steal personal information that is stored in or with these objects, yet they sometimes never make use of the personal information. It has recently been reported that during the past year, the personal records of nearly 73 million people have been lost or stolen, but that there is no evidence of a surge in identity theft or financial fraud as a result. Even though any loss or theft of personal information is troubling and potentially devastating for the persons involved, a strategy to keep consumer data out of the hands of criminals is essential.

Second, a thief attempts to misuse the information they have acquired. At this stage, criminals have acquired the victim's personal information and now attempt to sell the information or use it themselves. The misuse of stolen personal information can be used by thieves to obtain account information involving credit, brokerage, banking or utility accounts that are already open. This is a very common form of identity theft. For example, a stolen credit card may lead to thousands of dollars in fraudulent charges, but the card generally would not provide the thief with enough information to establish a false identity. Moreover, most credit card companies, as a matter of policy, do not hold consumers liable for fraudulent charges, and federal law caps liability of victims of credit card theft at $50 (FTC, 2010).

Offenders use personal information, such as Social Security numbers, birth dates and home addresses to open new accounts in the victim's name, make charges indiscriminately and then disappear. This type of identity theft occurs when thieves steal as much information as they are able to from burglaries or by hacking into a victim's accounts, which results in much greater costs and hardships on the victim. In addition, identity thieves sometimes use stolen personal information to obtain government, medical or other benefits to which they are not entitled.

Thieves commit their crimes and then move on to cash in on the benefits, before victims become aware of the extent of damage that was done to their name. These actions will eventually force some victims to suffer loss of employment and possible government assistance.

(iv) The Organized Crime Identity Theft 'Horizon'

As interviews with offenders progressed, a growing awareness emerged of the extent to which the individualistic model under which they operate is expanding to much broader dimensions due to the increased involvement of organized crime in identity theft. Therefore, a secondary level of research into case records was deemed necessary in order to gain insight into what the offenders were referring to (with most of this data coming from investigatory work as well). Therefore, some identity theft cases involving rings run by organized crime are reviewed.

New York City has been referred to as the crossroads for identity theft because it is one of the most populous urban areas in the world with approximately 8.3 million-plus residents within 301 square miles. The City exerts a powerful influence worldwide with finance and commerce. In 2008, there were 47 million visitors, which reflected an economic impact of $32.1 billion (nycgo.com 2010.) On a daily basis, there is a high volume of monetary transactions that are carried out in New York City; as a result, the City becomes a breeding ground for identity theft. Therefore, it becomes an alluring trade for the fraudsters who operate in organized groups.

The end of prohibition in the 1920s gave rise to organized crime in the United States. The Italian Mafia was one of the first crime syndicates to operate out of New York City under strict Mafia codes. In the 1990s Russian organized crime groups became more prevalent in New York City where they solidified their roots and operated primarily in the Brighton Beach, section of Brooklyn. Operatives within those groups were also traced to south Florida and California. NYPD confidential files in the Organize Crime Control Bureau (OCCB) reflect approximately

18 different organized crime groups with ties to Lithuania, the Ukraine and Armenia. According to the OCCB files, there are approximately 800 criminals who have infinite resources and escape routes to countries with no extradition treaties. This allows them to launder large sums of money, smuggle drugs, become active in immigration fraud, identity theft, human trafficking, prostitution, stolen vehicles and murder; they operate more loosely than traditional organized crime groups because they are not bound by strict rules and regulations. Undercover detectives have been challenged to put the fraudsters out of business because of limited resources, a lack of familiarity with the culture and the reluctance of victims who are too afraid to report crimes.

The victims fear the organized crime groups more than they fear the criminal justice system. Most of the victims have families back in their home countries that they are unable to protect because the crime leaders and their associates within the organized groups maintain records on the families. The victims have a dilemma hanging over their heads. The OCCB report refers to the gangsters as “true organized crime criminals” who are dangerous and fearless and are not afraid to offer a mere $10 to $20,000 for one to carry out a murder. On the other hand, Collins (1988:412) presents two conceptions of how individuals are bonded together in larger social structures. There are the connections between networks and markets or exchange theories.

Although identity theft is defined in many different ways; it is fundamentally, the misuse of another individual’s personal information to commit fraud. Identity theft continues to expand and adapt through several life cycles and continues to be a formidable task throughout the law enforcement and criminal justice world. Identity theft includes several levels of organisation.

Unlike traditional organised crime that is very structured and involves established lines of bureaucracy, identity theft can be fluid and at times disorganised. Some low-level fraudsters can be successful when stealing identities alone, yet others must be organised because

of the benefits that are reaped by networking with others. Some are involved with networks that operate in multiple states, while others were involved in gangs.

(v) West African Identity Theft Scheme

In May 2009, a very sophisticated and organized identity theft group consisting of Nigerians was broken up by investigators from the New York Police Department (NYPD) and the Kings County District Attorney's Office in Brooklyn. Approximately, $15 million was charged to 6,000 victims' accounts at several banks. Thousands of credit cards were intercepted by phony thieves just before those cards reached their legitimate destinations. The thieves then used Spoof Cards to disguise their voices in order to activate the cards. The thieves requested and were granted cash advances. They bought extravagant items in Saudi Arabia, Dubai and even Japan. Thirty-five Nigerians were arrested and charged with enterprise corruption, but interestingly enough, they were not charged with identity theft. A realtor from Queens, New York, mistakenly opened a postal package meant for another employee and found approximately 60 new credit cards. The realtor alerted police. This led to the opening of a full-fledged confidential investigation, which included wire taps. The cards were traced around the world by utilizing up to 80 wire taps, which helped investigators listen to $1 million phone calls. Because of the magnitude of this investigation, consultants who spoke various West African languages and dialects were hired as temporary employees to help transcribe the recorded conversations relevant to the investigation.

In 2005, a global security investigator received a call from a human resource representative at a large investment company in New York City, outlining a chain of illegal events at the company. This complaint was made utilizing the company's hotline. According to

e-mails that were received, the Compliance Report outlined suspected illegal and adverse company violations in the New York area. Mr. N., a compliance manager, identified the caller as former-employee Mrs. X who was hired as a New York sales representative until January 2005. According to Mr. N., he conducted a telephone interview with Mrs. X on May 5, 2005 and stated that Mrs. X was very open and willing to explain in some detail how this ("the scam") began and would identify some current and ex-company employees who were also involved. She did not know how long or who started the deceptive operation, but implicated current employee Mr. J, a sales associate in Indianapolis, Indiana and Mr. B, a sales representative located in New Jersey. Mr. J was terminated from the company on October 10, 2003. Mrs. X reported that Mr. J allegedly stole prescription pads from physicians' offices, forging signatures and using other bogus patient names to falsely obtain medication.

The prescriptions were accompanied by a 30-day performance Rx trial pack coupon. Sales representatives are given supplies for promotional purposes only. This illegal activity lasted for approximately 18 months and was witnessed by the caller on several occasions. Mrs. X also stated that Mr. J used the pads and received prescriptions from a pharmacy on Second Ave, on the Lower East Side in New York City and possibly other pharmacies. Mr. B allegedly used stolen script-pads belonging to Dr. A.M., who is located on Sutton Place, on the Upper East Side of New York City and forged scripts stolen from Dr. V to obtain the medication. All parties were arrested and prosecuted under the New York State Identity theft statute.

(vi) New Jersey/Florida Identity Theft Scheme

In September, 2009 United States Attorney Robert Kirsch, who represents the State of New Jersey, presided at a court hearing for Ronald Hyppolite, an admitted mastermind of an

identity theft ring. Hyppolite was originally sentenced in New Jersey for conspiring to steal thousands of credit reports. In 2003, he and his live-in girlfriend, Marie Louissaint, were both employed at a financial services and reality company that employed over 600 employees and were licensed to do business in almost the entire continental United States. Hyppolite persuaded Louissaint to steal copies of customers' credit reports. Information on those reports was used to hack into the company's internal computer system to lift clients' confidential financial information. He conspired with four of his receivers who sold the stolen credit reports and even used information from some of those reports to purchase over $2 million in computers, hand-held devices, other electronic merchandise and clothes.

In 2004, Hyppolite plead guilty to wire fraud and conspiracy. Due to his co-operation with authorities, Hyppolite was allowed to surrender to federal prison at a later date. Soon after he was out of court, Hyppolite fled to Florida with the help of some of identity theft-cohorts; he managed to evade the authorities and lived under the name, "James Present." The fraudster, while residing in Florida, assumed a stolen identity from the batch of identities that he still possessed. He lived as a fugitive under an assumed name in order to avoid a 4 ½ year prison term. Hyppolite's trade resumed as soon as he moved to Florida; he organised an identity theft ring that sold phony travel documents to unsuspecting victims who travelled primarily from Haiti to the United States.

(vii) The Kraft Foods Scheme

In May 2007, Manhattan District Attorney Robert M. Morgenthau unsealed an indictment against a gang of thieves who used several aliases to commit their crimes. The indictment showed that Latoya Gill, Anthony Hansen, Monique Clarke, Rafael Rodriguez, and Kesha

Robinson stole $200,000 by using the personal identifying information of hundreds of employees at Kraft Foods.

In the late 1990s, Monique Clarke, whose father was an auxiliary police officer, was a temporary consultant at Kraft Foods in the New York facility. During her sixth-month employment period, she had access to personnel records containing the personal identifying information of as many as 60,000 Kraft employees. The personal information of 600 employees was recovered after a search warrant was executed at a house where three of the defendants lived. Clarke obtained the personal identifying information of the victims and provided their personal details to other members of the identity theft ring. Gill and Hansen used photographs of Rodriguez, Robinson and others to create fake identification bearing the defendants' photographs which matched the stolen personal information of the identity theft victims.

Rodriguez, Robinson and others used the fraudulent documents and personal information of identity theft victims to open American Express credit card accounts at Costco stores in Arizona, California, North Carolina and Virginia. The defendants went on shopping sprees, purchasing merchandise, such as jewellery, electronics, laptop computers, cellular phones and food for re-sale and personal consumption.

For example, in February 2006, different members of the identity theft gang met at four different Costco stores in Virginia used fraudulent identification to open Costco memberships and American Express accounts and purchased merchandise costing $23,647.90, including three large screen televisions, an iPod, computers, Sony PlayStations, a prepaid cell phone, a camera and Dom Pérignon champagne.

In March 2006, the fraudsters started opening fraudulent accounts at several Costco stores in Arizona, purchasing merchandise valued at $61,528.70, which included a number of

diamond rings, Breitling watches, iPods, computers, flowers and liquor. The thieves continued this pattern of activity until June 2006, frequenting Costco stores in California, Virginia, North Carolina and Arizona, each time using similar tactics, opening fraudulent accounts and then purchasing expensive jewellery and electronics. Investigators discovered that from January to June 2006 the thieves stole Costco merchandise valued at over $200,000 using American Express credit cards. Their spending expedition came to a halt when one of the thieves was jailed in 2006 on an unrelated parole violation. The remaining gang of thieves was extradited from Virginia to New York, in order to face charges in court, including Monique Clarke, who was almost nine months pregnant at the time.

(c) Offender Profile

The profile developed of identity fraudsters both corresponds to and diverges from the profile developed in research. For example, Joe, Bobby and Michael had all participated in other forms of theft, and inadvertently entered identity theft as a spin-off from these efforts. Michael was unaware of the potential of stolen identity, and others moved on to identity theft because of the perception that prosecution was weaker. In one case, Fatima fits the model of an accomplice to an identity thief, that is, as a corrupt employee who sold information, but she exploited her own boss, stealing a credit card to finance a lifestyle. Thus, the claim that identity theft derives from former life in theft is generally confirmed, but with exception, meaning that persons without records may also become attracted by the ease of the crime.

Second, the findings indicated, from Jake and others, that few identity thieves could rationalize their crimes as victimless. Jake clearly knew that he was stealing from women, Michael's previous work as a pickpocket clearly constructed his victims as victims. In the case of the hotel worker dumpster diving and Fatima stealing her wealthy boss's credit card, however,

the social class divergence may lead identity thieves to rationalise their crimes by arguing that their victims as so rich it would not negatively impact them. Smith (2009) found that many identity thieves had skills in forgery, and other skill sets for exploiting stolen identity. This was not borne out by the interviews. No individuals espoused skill in forgery, all simply took the stolen information to illegal operations where the information was converted by others into forged credit cards, or, even less, simply sold their information for a forged card, and gained nothing from whatever else the forger did with the information. Only Harold seemed well informed on a particular scam using cell phone bills, re-routing mail, filing for a change of address card, and thus manufacturing new identities. Harold was also unique among the interviews in maintaining control of the second level of crime, selling the forged IDs to illegal aliens and shoppers, though he did not report if he gained a cut of the products sold by bodegas that then bought those stolen goods, in the third level of crime.

Third, it is apparent that credit card fraud still remains very important, with Jake stealing wallets for credit cards, Harold getting into identity theft through a credit card, but Harold focused on cell phone bills (presumably because they carried more personal information), while Jake reported that in robbing houses his crew would take "whatever I could find with their personal identifying information," and Bob reporting that in addition to taking credit cards, family photos, birth certificates, utility bills and "even whole drawers of paperwork" were taken, evincing a broader conceptualisation of personal information that went beyond the format-specific approach to findings found in current research. This awareness that all forms of information were exploitable perhaps represents a new threshold in identity theft crime. Joe seemed aware of this, but focused on a unique piece of information, almost as if it was his forte, a person's mother's maiden name (a common security question asked most people in most sites).

With regard to that key juncture where offline moves online as a site for committing identity theft crime, only Joe and Bob seemed aware of the possibilities of the online dimensions of their crime (everyone else selling their stolen information to others, who presumably then operated online). Joe surfed for websites which purchased illegal personal information, and made his money that way: that said he did not seem to pursue the Internet any further. Bob was aware of the bigger picture when he brought the stolen information to persons who processed it out to make IDs and then use then to hack into websites and gain credit reports.

Fourth, supporting the research of (Berg, 2006), Jake and Michael gained access to personal information by stealing wallets, while the hotel-employee thief gained stolen information from 75 guests at the hotel by dumpster diving. While the theft of confidential paperwork was lower down on the list of targets in the model formed thus far by research, it would appear that this is changing and confidential paperwork being increasingly viewed as exploitable, with Joe, again, fixating on the mother's maiden name as a bit of information that opened up welfare, food stamps, fake IDs and other crimes from it. While corrupt employees are also understudied by research, both Fatima and Dave the hotel employee, but in this case both working for them, were gainfully employed, and went bad. No respondent mentioned buying illegal information from employees of companies. No respondents reported being involved in phony mails, or in any form of scam telephoning. In terms of motivation, Jake stole information to make some money, as did Michael, and Joe, with little greater ambition. Bobby stole to contribute to a gang, which in turn converted the stolen identification into credit cards used by other members to purchase luxury goods, which were then sold overseas. As Michael came to gain insight into the mechanics of what is done with stolen information he gained a fake credit card and used it, more or less, only to finance his own lifestyle, renting a single occupancy hotel

room to keep his lifestyle going. No respondents reporting writing false checks, using fake IDs to gain employment and none sought to create a new life for themselves. Overall, then, the individual offenders interviewed here present themselves as low-end single operatives working with a limited knowledge of identity theft and its potential, undertaking basic information theft, then selling their stolen information for a quick, minimal profit, to others, who then exploited it for larger purposes. While only Michael seemed to be becoming aware of the wider potential of his crime, Bob and Joe, working in gang or organized crime situations, while not individually profiting from their transfer of stolen identity to others, who then converted it into second and third spin-offs of crime, had a higher awareness of the organizational or systemic potential of identity theft.

From this result, it is suggested that the current model of identity theft is overly focused on the theft aspect of the crime, and not on the levels of fraud which develop from the original theft. That is, a theft then involves a sale, which then involves a forgery, which then involves illegal purchasing and exploitation of the forged instrument, which then involves sale of the products illegally purchased, a spiral of crime that appears limitless and understudied by the current identity theft models. Most of the respondents in the interviews in this study were engaged in identity theft, they only gained limited insight into the dimensions of identity fraud (not to mention the international dimensions of their original small crime). Finally, the notion that identity thieves view their crimes as victimless cannot be supported: they know that they are victimising people. They may only rationalise it as stealing from the rich to give to the poor (themselves). Finally, one hundred per cent of the respondents in this study reported that they had replaced their material goods theft life with identity theft.

(i) Routine Activities Theory

With regard to routine activities theory, the reports by respondents more or less confirm the model. That said there were a few elements of routine activities not borne out. Routine activities theory argues that offender motivation is partly fueled by the least amount of effort in committing a crime. In the case of Jake, who would sleep with two women a night, the hotel employee, who dumpster dove after hours, Michael, who undertook a rigorous daily routine of subway pick pocketing, and Bob, who engaged in meticulous and relentless casing of suburban homes, all engaged in enormous effort to get the information they needed, meaning that they were motivated by its current value more than anything else.

Routine activities theory does state that the physical weight or portability of the target is a determining factor, and it is certainly true that most respondents appreciated theft only involving wallets, cards, and, even more portable, paperwork. The current research on identity theft, in accordance with most laws, seems to have fixated on formats of information, especially credit cards or debit cards. But Bob and Jake especially seemed aware that personal information of all sort was exploitable: thus, there seems to be a growing awareness that it is not about the format but about the information in the abstract. In this regard, the most eye-opening paradigm-changing observation was made by Bobby, burglar of suburban homes, who indirectly indicated that whereas formerly he might have paused to lift a television, electronics, jewelry, or other goods, to be later fenced, the focus of his gang today was to go right past these to personal information, of any kind, to the extent that they would take on the added tasks of lifting whole drawers of paperwork. Thus, a conventional crime is transformed by the focus on identity information into a new crime. The further de-materialisation, as it might be called, of identity theft, was evinced by Joe's fixation of the mother's maiden name, and all of the false paperwork that it can generate. Where this awareness ends up is that all one needs is names, numbers, secret

coded data, and not the physical elements: one can "steal" from a debit card that still resides safely in a consumer's wallet, no crime apparently committed, by allowing an associate to pay for an overseas hotel room with the stolen number.

Also with regard to routine activities, it appeared that most respondents exploited people going about their daily lives, on subways, going to work, staying in hotels, and going out at night. In the case of Jake, who went home with women, and Bob, who posed as a delivery boy or gardening, criminal intent was disguised under routine business that would disqualify the oversight of either neighbours or police. It would appear that in all aspects of daily life, most people, by continuing to carry multiple pieces of ID in wallets, by not securing personal information in their homes, by tossing out credit cards slips in hotel dumpsters, by carrying PINs and Social Security Cards in wallets, continue to be generally unaware of the full dimension of identity theft. Finally, the overwhelming aspect of routine activities theory validated by my interview-based research was lack of preventive guardianship. One hundred per cent of respondents reported that they got into identity theft because there is little chance of being caught, or, if caught, much less punishment. This impunity was expressed on many levels, observing little detection on site (though Michael was apprehended on a subway), little chance that, if reported, police could conduct an investigation in a timely manner (though the hotel employee was eventually apprehended by a hotel guest who reported the theft), the grey areas of police jurisdiction in the overseas dimensions of the crime, the laxity of the judicial system, and the fact, as Joe mentioned, that even in prison, a paper-based crime like identity theft can continue to be conducted. As a result, it has to be concluded that at present, according to routine activities theory, a perfect storm of high offender motivation, high suitability of target and low level of

guardianship has made identity theft the crime of choice, and likely to be the crime that more criminals move into.

(ii) Beyond the Individual

Finally, another dimension entered into the picture briefly, in my individual interviews, which then led me to a broader study of the full scope of identity theft, that is, the involvement of organized crime. In the case of Joe and Bob, their involvement in gangs or organized crime, meant that they had much more sophisticated view of identity theft as it morphed and expanded into identity fraud. Identity theft could be defined as efforts undertaken to steal the personal data, while identity fraud can be defined as all efforts undertaken by associates and others to exploit the stolen information, involving forgery, obtaining false documents, filing for fraudulent funds, welfare checks, food stamps, illegally purchasing merchandise, selling that stolen merchandise to other merchants, or overseas: fraud is the dimension where "identity theft" as a crime appears to be in danger of exploding to "intermestic" dimensions far beyond the capacity of location-based law enforcement agencies to manage or combat. As a result of this conclusion, some additional research was conducted into the scope of organized-crime run identity fraud rings, and the findings confirmed that identity theft continue to develop through several cycles of crime, and even become involved in other kinds of gang crime, to become a significant stream of organized crime criminal behavior. In relation to this the research has identified corrupt employees as often being found to be a source for thieves to obtain stolen information. While little evidence was found of this in the testimonies of individual identity thieves, placing an employee in a company or organization emerges as the primary means by which organised crime rings of identity fraud originate. This makes the numbers of persons exposed to identity theft increase exponentially: while the hotel employee might have been proud of himself to have amassed 75 identities in his

possession after weeks or months of arduous dumpster diving, employees routinely have access to the personal information of hundreds of employees (in one case, 600), vastly expanding the dimension of fraud (and, of course, still much greater numbers have been publicized in cases of laptop theft and hacking of bank accounts in the press). This high volume of conversion also necessitates high volume of gang members to then exploit the information: while Bobby might have been impressed that his small gang was able to train a few woman to go to NYC department stores to illegally purchase luxury goods, focused identity theft gangs can range over many different sites simultaneously, conducting a much higher volume of illegal purchase.

Also, organised crime identity fraud rings are much more aware of the potential of pure document-based information, as opposed to its format on credit or debit cards, and enact their crime much more quickly and more often in online as opposed to offline environments. That is, organisation moves the crime from identity theft to identity fraud at a highly accelerated rate. In a way, then, this study found, starting with individual identity thief testimony, that just as they were surprised at, but still primarily in the dark about, the organisational dimension and potential of identity theft, so the current paradigm of law enforcement, as well as the legislation and research literature, focused on identity theft, is in more or less the same situation, only beginning to become aware of the widespread dimensions of identity fraud. At present, precinct police no longer even know how to fill out a police report for identity theft, as, while the crime may have been detected by a bank customer at a bank in their precinct becoming aware of suspicious activity in his account, the actual crime, making use of a number not a physical debit card, occurred overseas, which means that "there is nothing we can do." The conclusions of this study of offender motivation therefore finds that not only is it high, but that as offenders become more aware of the systemic potential of the crime, and identity theft morphs fully into identity fraud,

not foreseeing systemic law enforcement response, offender motivation will continue to remain high for the foreseeable future.

Statistically, the findings of the chapter on offender motivation, with regard to stolen ID, is that 28 (23.3%) used stolen ID to obtain credit, 22 (18.3%) made use of the stolen ID to hide their true identity, 19 (15.8%) used stolen ID to obtain government documents, 16 (13.3%) used stolen ID to open bank accounts, 13 (10.8%) used stolen ID to purchase large ticketed items in stores, 12 (10%) sold stolen ID documents to undocumented aliens and 10 (8.3%) sold stolen ID documents to gang members. At present, this motivation list continues to demonstrate that the majority of ID thieves continue to make use of stolen ID for personal reasons, and only to a lesser extent convert stolen ID into other documents that lead to greater and other crimes. Moreover, the organized nature of ID theft, characterized by simply selling stolen ID to other criminals or undocumented aliens, while a growing motivation, has not yet superseded personal use of stolen ID by fraudsters.

Some comments on offender motivation

Overall, the interviews with offenders raised a broader issue, linked to routine activities theory and the situational crime prevention paradigm, as to offender motivation. In this, routine activities theory is situated in an ongoing debate over the nature of offender motivation. The paradigm is grounded in the basic notion that offenders who are willing to commit crimes think with a limited rationality and are affected by the perceived benefits and costs of their actions. Formerly it was believed that offenders were motivated by greed and a lack of self control even though they are not necessarily concerned with taking risks and the type of consequences that they may encounter. But bounded rational choice theorists recognise that humans are limited in the amount and kind of information they are able to process, the amount of information they are

able to store, and how the information gets processed and interpreted—but nonetheless calculate costs and benefits with what information they have at hand. This, then, is the notion of bounded or minimal rationality (Simon, 1957). This theory is, in turn, the basis of the situational crime prevention paradigm and routine activities theory.

Therefore, the identity thief decision to offend is, indeed, influenced by situational considerations as to how accessible a crime target will be and how quickly his escape can be made. In addition, the existence of security mechanisms or the likelihood that a victim could be armed or resist also plays a role in offending. The profitability of the corporation and size of their account also plays an important factor in most fraudulent crimes. By accounting for the efficiency of the goods, the offenders are cognizant of gaining the support and loyalty of their customers and of those who are willing to fence the illicit goods. The offender's rational choice approach considers the alternatives available, including, moving the goods in a cost-benefit manner so as to benefit from the profits. This method tends to evaluate the effectiveness of the scheme by way of their profit margins. As the rational choice theory becomes more dominant, supported by a process of normalization created by the spread of identity theft into organised crime, a complete self-sufficient base has been established to support the culture.

Therefore, we must accept the implications of identity theft in both theory and policy. The individuals seek their objectives because of self-interest and the expected benefits that their illicit behaviour will produce as compared to the limitations of lawful employment. There is a risk factor that the criminal will weigh to determine if his activity is worth more than the punishment if caught. Most offenders would carefully calculate the advantages versus disadvantages of committing a crime. My research shows that this behaviour encompasses all ethnicities, educational levels, ages and gender. The only individuals who really seem to be

affected by current risk factors are those offenders with criminal records who realise the ramifications when caught by law enforcement.

Identity theft fraudsters are aware of stricter laws for offenders for incarceration for other crimes. The cost of offending includes, but are not restricted to, the possibility of severity of formal legal sanctions. Other costs also include the certainty and severity of informal sanctions and moral costs such as loss of respect and shame. At present, this is not the case in identity theft. Katz (1988) believes that some offenders view crime with excitement, as an activity to engage in a fun way. Today's society emphasizes high living, partying and "keeping up with the Joneses," possibly reinforcing these views. As one of my offender interviewees stated, "I can't see myself working at McDonald's for minimum wage when I can make easy money ripping off someone's identity." The current laws aimed at identity theft have little or no effect deterring thieves. Additionally, the sentences imposed on offenders do little to prevent them from thinking about re-offending in the future and even to recognise the severe burden that victims face throughout their daily lives. Even though identity theft can be perpetrated on a trans-national level, there are at present no set mechanisms in place to prevent such activity. The judicial system and the private sector do not share the same views and are less likely to educate each other and partake in necessary security controls which may lead to a more aggressive prevention technique against identity theft in the future. If, however, corporations and the judicial system recognised the seriousness of identity theft and would be willing to publicly acknowledge this serious threat, increasing the prosecution of this crime, offenders will be forced to alter or change their attitude about the crime. In doing so, combined with an effective public and educational crime prevention campaign, the reduction of identity theft may be the result (Johnson and Bowers, 2003). The position adopted in this research is the virtue rational choice approach to the

problems of identity theft violence; therefore, it gives a methodological conceptual framework on the basis of which some understanding of the crime can be developed and offers avenues along which initiatives to effect change can be empirically explored.

Overall, the interviews with offenders raised a broader issue, linked to routine activities theory and the situational crime prevention paradigm, as to offender motivation. In this, routine activities theory is situated in an ongoing debate over the nature of offender motivation. The paradigm is grounded in the basic notion that offenders who are willing to commit crimes think with a limited rationally and are affected by the perceived benefits and costs of their actions. Formerly it was believed that offenders were motivated by greed and a lack of self control even though they are not necessarily concerned with taking risks and the type of consequences that they may encounter. But bounded rational choice theorists recognise that humans are limited in the amount and kind of information they are able to process, the amount of information they are able to store, and how the information gets processed and interpreted—but nonetheless calculate costs and benefits with what information they have at hand. This, then, is the notion of bounded or minimal rationality (Simon, 1957). This theory is, in turn, the basis of the situational crime prevention paradigm and routine activities theory.

Therefore, the identity thief decision to offend is, indeed, influenced by situational considerations as to how accessible a crime target will be and how quickly his escape can be made. In addition, the existence of security mechanisms or the likelihood that a victim could be armed or resist also plays a role in offending. The profitability of the corporation and size of their account also plays an important factor in most fraudulent crimes. By accounting for the efficiency of the goods, the offenders are cognizant of gaining the support and loyalty of their customers and of those who are willing to fence the illicit goods. The offender's rational choice

approach considers the alternatives available, including, moving the goods in a cost-benefit manner so as to benefit from the profits. This method tends to evaluate the effectiveness of the scheme by way of their profit margins. As the rational choice theory becomes more dominant, supported by a process of normalization created by the spread of identity theft into organised crime, a complete self-sufficient base has been established to support the culture.

Therefore, we must accept the implications of identity theft in both theory and policy. The individuals seek their objectives because of self-interest and the expected benefits that their illicit behaviour will produce as compared to the limitations of lawful employment. There is a risk factor that the criminal will weigh to determine if his activity is worth more than the punishment if caught. Most offenders would carefully calculate the advantages versus disadvantages of committing a crime. My research shows that this behaviour encompasses all ethnicities, educational levels, ages and gender. The only individuals who really seem to be affected by current risk factors are those offenders with criminal records who realise the ramifications when caught by law enforcement.

Identity theft fraudsters are aware of stricter laws for offenders for incarceration for other crimes. The cost of offending includes, but are not restricted to, the possibility of severity of formal legal sanctions. Other costs also include the certainty and severity of informal sanctions and moral costs such as loss of respect and shame. At present, this is not the case in identity theft. Katz (1988) believes that some offenders view crime with excitement, as an activity to engage in a fun way. Today's society emphasizes high living, partying and "keeping up with the Joneses," possibly reinforcing these views. As one of my offender interviewees stated, "I can't see myself working at McDonald's for minimum wage when I can make easy money this way." each other and partake in necessary security controls which may lead to a more aggressive prevention

technique against identity theft in the future. If, however, corporations and the judicial system recognised the seriousness of identity theft and would be willing to publicly acknowledge this serious threat, increasing the prosecution of this crime, offenders will be forced to alter or change their attitude about the crime. In doing so, combined with an effective public and educational crime prevention campaign, the reduction of identity theft may be the result (Johnson and Bowers, 2003).

(d) Conclusion

This chapter summarised the findings of interviews with offenders of identity theft conducted as part of this study. The results were then compared with a rubric of current understanding as it exists in the research reviewed in Chapter 2. The fact that offender response opened up the dimension of organised crime involvement in identity theft also led to additional research focused on that aspect of the crime, and some less-detailed interviews with those involved. Overall, the results found that offender response to identity theft, in terms of their motivation for doing it, their sense of the suitability of the target, and their sense of the absence of guardianship, conforms fairly well to routine activities theory. That is, from the point of view of offender response, routine activities theory would appear to have a high degree of explanatory power in explaining offender involvement, and also suggests ways to curtail their current level of freedom. With regard to the research, offenders response often corresponded to general findings,especially with regard as to the continued importance of credit cards, and mechanisms of crime including theft and dumpster diving, but at the same time offender response strongly suggested that identity theft has taken on a contagious or viral quality that is spreading to many different opportunity occasions including an increasing number of employees of any number of

industries or workplaces who are being lead into identity theft by the opportunities presented them by lax security.

The offender response also indicated that by and large the identity thieves currently apprehended by NYPD and others, though this is changing, are the small-time original offenders who then more often than not pass on their stolen IDs to others who, as part of more organised operations, make most of the money from the crime. That is, just as offender response indicated a growing awareness of the size and scope of the crime, so too their responses contradicted the current research by indicating a growing trend toward involvement of organised crime in identity theft, and a persistent movement from offline to online commission of identity theft crime, for the purposes of increasing the offender motivation by gaining a 'bigger bang for the buck' in the crime. Finally, offender response also strongly suggested, simply, again, by a dawning awareness in offenders as they grapple to understand the implications of all that they have done, that the particular means by which information is carried, such as credit cards, or debit cards, is becoming less important to focus upon as personal data in general, and, in particular, elements of personal data asked for by security systems online, including, for example, Joe's fixation on the 'silver bullet' quality of having a victim's mother's maiden name in his possession, which opened up so many other possibilities for fraud, extending to the obtaining of false documents, selling them to illegal immigrants, and other uses. Overall, while on the low end of the continuum focused on original identity theft crime offender response and the research generally compare, as one moves to the high end of the continuum, and from offline to online, divergence between current research and developing practice is greater and, likely, ever widening.

CHAPTER 6: Impact of the Criminal Justice System

(a) Introduction

This chapter will present the findings relating to research question five, namely what have been the strategies of the executive and legislative branches of government, including law enforcement, to address identity theft and what challenges do they continue to face in their effort to detect, investigate and combat identity theft? The findings presented are based on research literature and on the interviews with law enforcement stakeholders. The results expand upon the definition of identity theft and the appraisal of the role of the internet in its commission, and consider the gap between theory and practice in identity theft activity. The method of this chapter is the same as in chapters four and five, with some differences to account for confidentiality issues. The chapter will present the results of interviews with stakeholders and compare them to the existing research findings as well as to routine activities theory, based on instruments utilized to guide the interview. An added dimension of this chapter is that, having gained a sense of offender and victim perception of law enforcement effectiveness, these findings can also be compared to the self-perception of law enforcement. Therefore, the purpose of this chapter is to determine if the perceptions of stakeholders in law enforcement, criminal justice, and affected businesses correspond with these views of ineffectuality, if law enforcement perceptions exceed or lag behind research, or take routine activities theory into consideration, and if offenders and victims are correct in viewing law enforcement response as ineffective.

In order to achieve these ends, first, a brief review of the United States government response to identity theft as embodied by legislation will be made. Second, a general impression

of interviews of investigators, law enforcement personnel and officials, and other stakeholders involved in identity theft will be drawn, taking confounding factors into consideration. This chapter chooses a general summary approach to most interviews, rather than detailing interviews as in previous chapters, due to the higher constraints upon confidentiality, as indicated by the high profile of confounding factors in this part of the research, when dealing with personnel whose identity could be discerned by reference to rank and department, regardless of the use of anonymity. Third, variables in levels of awareness as they contribute to current investigation of identity theft will be addressed, with particular focus on the greater willingness of higher-level law enforcement officials and criminal justice stakeholders to address identity theft when it escalates to the organized crime dimension. Indeed, while some awareness of the organized crime dimension of identity was gleaned from offender response, the bulk of data obtained about this expanding scope of identity theft was extracted from the study of cases and responses of investigators involved in these cases. Therefore, even though research inside the investigatory side of identity theft was often confounded, it also resulted in the keenest insight into the inner workings of organised-crime-level identity theft.

(i) Governmental Response to Identity Theft

With regard to research question five, what have been the strategies of the executive and the legislative branches of government (the criminal justice system), including law enforcement, to address identity theft and what challenges do they face in their effort to detect, investigate and combat identity theft, both of review of literature research and a follow-up review of primary documentation were undertaken, and compared, to determine the state of the art in legislative and company response to identity theft.

(ii) Legislature and Private Company Response

A review of the literature generally found that response to identity theft by law enforcement has been limited by existing paradigms, inherited from legislative response, which have therefore also limited the effectiveness of combating identity theft online. At present, as mandated by legislation (see below), most companies self-enforce red flag rules for the detection of account irregularities that may indicate that identity theft is being undertaken (Bose & Leung, 2009). Red flag rules were imposed upon companies by the Federal Trade Commission in 2007. In addition to Red Flag rules, breach notification rules have been required for the 'other' side of identity theft, that is, when an identity theft incident is detected and companies therefore must inform consumers (Burdon, 2011). The rationale behind breach notification rules is that informing a consumer quickly of an attempt at fraud will allow them to react in a way to prevent further damage. The rules had to be imposed because some companies were reluctant to advertise the fact that their systems had been hacked or in other ways compromised. Companies also undertake training and employee awareness building efforts to improve the detection of red flags signalling identity theft and the submission of breach notification to consumers. In addition, the research found that by and large these protections have only been introduced over the past five years, meaning that many companies continue to evolve in the full development of red flag rules. By and large, the research has found that both red flag rules and breach notification laws have resulted in modest success in at least reducing the overall damage resulting from identity theft (Burdon, 2011). That said, a good number of researchers have criticized both the red flag and breach notification approach that is primarily reactive in nature, happening after the fact, and therefore not directly addressing the problem of the high incidence of identity theft attempts (Lee,

2009). The fact that both kinds of laws have been easily circumvented by phishers and hackers, so that a breach can be made without a red flag being detected, and therefore no breach notification is made until it is too late, is a second reason why researchers believe that this approach is limited in its effectiveness (Garrie et al., 2010). Glithero (2009) also pointed out that the Identity Theft Penalty Enhancement Act of 2004 has been interpreted in so many different ways that it has lost its effectiveness.

The research also indicated that in addition to red flag rules, companies have addressed identity theft with technical solutions. These include adding encryption, content-monitoring and content-filtering methods, and introducing a number of software-based and technical advances that will counteract phishing and other online fraud methods (Computer, 2009). Here, too, however, impressive though the technical defences developed by information technology departments may be, it is the consensus of research that this approach only enmeshes companies in an identity theft arms race that they cannot win, as phishers and hackers are able to counter any technical defences in fairly short order, making the work involved in devising the technical device worthless quite quickly. It should be noted that while the research tends to discount the effectiveness of both red flag rules and breach notification laws, in the testimony of victims of identity theft covered in this study both red flag rules and breach notification laws emerged as the only moving parts in the identity theft crime-fighting effort that appear at present to work well, if not to prevent the crime from happening, then at least to minimize the negative outcomes for the consumer. In several cases studied (see chapter 4), lacking red flag rules and breach notification laws, the size of the crime committed against victims would have been much larger,

and, in all cases, the quickness with which the crime is detected is of critical importance in minimizing the damage of the crime done to a bank account and to the victim's emotional state.

Because of the relative ineffectiveness of both the red flag rule-breach notification reactive paradigm and the technical defence 'arms race' paradigm, research into identity theft has moved to favour a more preventive approach. Tilley & Kennedy (2009), among others, argued that a holistic criminological model such as the situational crime paradigm and the routine activities theory, insofar as this approach addresses preventive measures that can be taken before the crime of identity theft occurs, might well offer a more effective way to combat identity theft. Therefore, research has recommended the application of routine activities theory to the prevention of a number of different kinds of crime (Miethe & Sousa, 2010), leading this study to seek to apply this paradigm to identity theft.

(iii) In-depth Primary Documentation Study of Legislative and Company Response

In addition to reviewing the research literature on governmental legislative response to identity theft, this study also reviewed the laws themselves, to determine both how legal response to identity theft has evolved and the current status quo. The purpose of this separate examination of documents was to compare a specialist researcher's appraisal of the law, in the form of primary documentation, to the research literature's appraisal of the adequacy of the law. This review focused on seminal laws only, on the Federal level, and in the State of New York. At present, it will be assumed that how laws are created and passed in the legislature in both the United States and the State of New York is known, or can be researched elsewhere. It is important to know that several of the agencies mandated to manage identity theft are part of the executive branch, including the Board of Governors of the Federal Reserve System, The Federal

Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, and the Office of the Comptroller of the Currency and the Office of Thrift Supervision. The most significant landmark legislation identified in the research review was the 1970 Fair Credit Reporting Act, amended in 1996, but identity theft was not identified as a crime until the passage of the False Identification Crime Control Act of 1982 which prohibited fraud in connection with identification of documents and mailing of private identification documents without a disclaimer. The Act also prohibited the production and processing of devices which made or forged documents, but the law proved to be ineffective because it was overly focused on physical documents and not on electronic forms of identification.

A speech by James Bauer of the United States Service before Congress in 1998, emphasizing the fact that identity theft was spiralling out of control, lead to the passage of the Identity Theft and Assumption Deterrence Act of 1998, which penalized offenders who committed or attempted to commit identity theft. The law greatly expanded the various circumstances that would be now be considered identity theft, including any participation in the transference of stolen identity, including producing false identification documentation, transferring documentation known to be stolen, possessing stolen documents with intent to use unlawfully, possessing more than five documents with intent to transfer unlawfully, possession of even a single stolen document, or document that appeared to be (that is, possibly forged), issued by the United States and possession of any document-making implement either to create false documents or with intent to produce false documents, or even attempting to do any of the above. It was also a landmark in that it focused on consumers as victims for the first time, providing for the Federal Trade Commission to educate consumers and open a bureau to receive consumer complaints of identity theft. By greatly expanding, and specifying, the extent to which a person

could be prosecuted for even indirect involvement in an identity theft ring, this law was the first to give a more comprehensive form to anti-identity theft legislation.

By 2003, however, another round of offender and victim testimony before Congress focused on the fact that the new availability of credit had provided a new occasion for identity theft, which must be addressed. This resulted in the passage of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act), which not only reauthorized the Fair Credit Reporting Act of 1970, but was the first act to create Red Flag regulation in addressing identity theft. Red Flag regulations were imposed on companies to notify the Consumer Reporting Agency if any red flags indicative of fraud, primarily involving suspicious looking documentation, suspicious persons providing the identifying information, unusual or suspicious account activity, and any notices received from consumers or other parties involved that they were suspicious of activity, were detected in the operation of their business. Subsequent to this act, the Identity Theft Penalty Enhancement Act (109-275) increased the criminal penalties for violation of identity theft laws, the Identity Theft Enforcement and Restitution Act of 2008 (Title II of P.L. 100-326) which mandated victim compensation for identity theft by banks and other institutions, the Social Security Number Confidentiality Act (P.L. 106.433) which prevents the visibility of social security numbers on or through unopened mailings and the Internet False Prevention Act of 2000 (P.L. 106-578) which dealt with persons making false identifications. All of these acts are partial, and directed at specific problems as they arise and are observed. Inactivity on 46 other pieces of legislation indicates that as more problems are discovered, new proposals for legislative amendment are made, but Congress is reluctant to act.

As for the state law, the case study chosen in this research was New York State. Prior to 2002, prosecution of identity theft was done on an ad hoc basis by utilizing exiting laws such as

Offences Involving Computers (156), Forgery and related offenses (170), Criminal Facilitation (115), Larceny (155) and Offences Involving False Written Statements (175). With 7,076 complaints regarding identity theft as part of larceny and fraud, making New York only second behind California in instances of identity theft, lobbying was undertaken to have the New York State Legislature enact a law identifying identity theft statute in 2002. Under the New York State Penal Law, a person is guilty of identity theft in the third degree when he or she knowingly and with intent to defraud assumes the identity of another person by presenting himself or herself as that other person, or by acting as that other person or by using personal identifying information of that other person, thereby obtaining goods, money or property or uses credit in the name of a person to cause financial loss, or commits a class A misdemeanour or higher level crime. If the amounts involved exceed $500 this becomes a second degree offence, while first degree felony offenses develop when the amount exceeds $2000. The law also considered unlawful possession of false personal identification information in a wide range of circumstances or types including a person's financial services, account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, automated teller machine number or code, automated teller machine number or code, personal identification number, mother's maiden name, computer system password, electronic signature or unique biometric data that is fingerprint, voice print, retinal image or iris image of another person. Again, third, second and first degree offences were considered, as was prior arrest record for identity theft, and age, with special provisions for minors using false identification to purchase alcohol, for example.

What is impressive about this law, again, is the scope of the types of identification included, such as personal identifying information entails a person's name, address, telephone

number, date of birth, driver's license number, social security number, place of employment, mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, brokerage account number or code, credit card account number or code, debit card number or code, automated teller machine number or code, taxpayer identification number, computer system password, signature or copy of a signature, electronic signature, unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person, telephone calling card number, mobile identification number or code, electronic serial number or person identification number, or another name, number, code or information that may be used alone or in conjunction with other such information to assume the identity of another person. The inclusion of an electronic signature looks to be a breakthrough in identity theft prosecution, as it addressed a primary means by which identification is communicated on the Internet. Again, New York State, following Federal law, also found that affected persons were often exposed to more jeopardy and hindered in their efforts to find out about breaches of identity and take action because they received no notification. Therefore, in line with Red Flag acts, but addressed to consumer victims, the Technology Business and Commerce-Information Security Breach and Notification Act created an advocate for identity theft victims, mandated banks or companies to notify consumers of a breach, and made more provision for compensation. If New York residents have to be notified at one time, the person or business is required to notify the state Attorney General, the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure co-ordination as to the timing, content and distribution of the notices and approximate number of affected persons. Other laws were more specific. In 2003 the state legislature amended section 520-a of the General Business law by adding article 30-b to prohibit printing of more than the last five numbers of a credit card or debit card on a receipt, and

that all machines placed into service on or after January 1, 2004 must conform to this new section. All machines at least prior to January 1, 2004 had until January 1, 2007 to conform. Also, relevant in this law is subdivision 5 of section 520-a, which was amended as well to include penalties for violations with a cap of $1,000 per day, aggregate penalties added. Businesses that are in violation of these provisions are given two weeks' notice to correct the violations. If not, the penalty is $500 and the violator will be granted another week to correct the violation. If the violation is not corrected within that one week period, a penalty of $1000 per week is imposed until the violation is corrected, with a maximum not to exceed $4500 for violations occurring on the same premises.

(iv) Private Sector response

In addition to conducting an in-depth or focused research into legislative response to identity theft, this study also addressed specific efforts by industry, directly, to address identity theft issues. This research was conducted by attendance at industry conferences and perusal of primary documentation resulting from such conferences. From this research, it is apparent that the financial services industry is leading the way in addressing identity theft, undoubtedly since identity theft is targeted at their business. A round table event sponsored by BITS/Financial Services in 2009 reviewed all legislation passed to combat identity theft at the state and federal law and concluded that significant actions were still needed to address identity theft. The financial services industry in particular identified a number of industry-specific challenges remaining in their efforts to combat identity theft, including lack of field examiner support of new regulations, lack of high-quality field examiners, differences over law interpretation between authors of regulations and examiners, lack of shared insights between institutions, lack of clear, concise and timely communication of new regulations to institutions, lack of inter

agency coordination in enforcing regulations, failure of agencies to maintain adequate knowledge base of developments in identity theft and need for more collaboration between regulators and agencies.

These and other points clearly indicate still another weakness of current regulation: many different points at which the deployment of regulation through field examiners breaks down because of lack of coordination and collaboration. Overall, some of the regulatory measures adopted by the financial services sector advance upon legislative response include obtaining insight from industry-specific institutions and vendors to devise policy, arguing that the regulation be risk-focused and not technology-specific or overly prescriptive. This should result in providing better training on issues such as authentication for investigators and empowering field examiners to help and train companies develop better understanding of and make better use of Red Flag rules (on the assumption that Red Flag rules are not being adhered to adequately). The financial services industry has also issued its own industry-specific regulations such as the Chip and Pin System, implemented in 2006, which provides for greater protection of personal identification numbers and prohibits the use of stolen cards without PINs. This proactive effort by the banking industry has been found to be successful because the chip has not been fully cloned by criminals. The result of a reduction of loss and stolen card fraud also indicates moderate success. However, one significant study concluded that chip and pin is actually broken. The University of Cambridge paper authored by Steven J. Murdoch, et al. (2010), uncovered a relatively simple way that a fraudster performs a man in the middle attack to trick the terminal into believing the PIN verifies correctly, while telling the card that no PIN was entered at all. It appears that the failure is significant for the industry and does have significant public policy implications. With typical credit card fraud the merchant and/or the individual for purchase is

not held liable for the fraud; liability lies within the banking institution. The financial/banking institution motivates the industry to incorporate the chip and pin concept because could eliminate its liability, saving them millions of dollars that result from credit card fraud. The United States financial institutions have been very reluctant to switch to this new EMV smart card. Some companies have begun to issue EMV cards. However, the reason for the technology by these financial institutions has less to do with risk and more to do with global acceptance of the EMV cards. The larger institutions still opt for signature card holder verifications while credit unions seem to be opting for PIN card holder verification.

APACS, the UK payments association (2006) announced that Chip and PIN has reduced fraud significantly in the UK since the issuance of cards began in February, 2006. This has created interest in the United States even though it appears that the system is flawed to a degree. The question will be whether the United States is moving in the Chip and PIN direction because of the protection against fraud or the realisation that companies/entities can shift the liability of losses as a result of fraud. A highly placed executive in security at American Express expressed the belief, however, that if chip and pin was used in the United States "it would be cloned in no time". Part of the reason for this is he sees a significant amount of dishonest employees in this country, which may not be as prevalent in the European Union. He stated, "AMEX spent a large amount of money testing Chip and PIN cards against hand-held scanners which they purchased for fewer than two hundred US dollars. Not only were the cards scanned and cloned without touching the individual's pockets and bags which bore their plastic cards, items such as: school identifications and passports were easily scanned". Such an experiment shows the unexpected risk that is undertaken by a fraudster and the vulnerability and consequences which lies ahead for

the victim. Visa has developed a plan, which shows, if a transaction using a counterfeit card is carried out at a merchant with a chip enabled terminal, liability will lie with a merchant acquirer.

(v) Conclusions Regarding Government Response

This separate in-depth examination of specific primary document legislation, as well as internal company or industry attempts to combat identity theft, found that legislative response to identity theft has been primarily piecemeal, reactive, and technology-specific and too often a series of targeted acts focused on specific aspects of identity theft amended to laws. It was also found that legislation has progressed into the Red Flag paradigm. Both Federal and State legislation involving identity theft then, at present, continue to seem inadequate. That is, examination of primary documentation did not yield any different conclusions that the appraisal of legislation currently espoused by the research community. The fact that no "czar" has been appointed to oversee all identity theft efforts at Federal or State levels remains a serious problem. This was confirmed by reports from the financial services industry on the host of problems plaguing regulator and field examiner interaction and buy-in to regulations, resulting in the "dropping of the ball" in the chain from passage of regulation to enforcement. As for private companies, their focus on risk as opposed to technology or specific crimes is promising, but in practice they have also taken to addressing specific problems. That said a promising aspect of action derived from specific industry is that, due to the international nature of most such corporations, it is far more likely that a global protocol for various aspects of identity theft will emerge from this source and not from either Federal or State legislation. These findings of some action on promising methods of prevention indicated a willingness of industry to move beyond the Red Flag paradigm in a way that advances upon current research: thus, in this case,

attendance at an industry conference and review of primary documentation and expert opinion yielded some degree of progression from the review of literature.

At present, however, a review of the current legislative and company response to identity theft can only lead to the conclusion, shared by the research literature, that identity theft remains, legally, a 'new crime' which the law still struggles to keep up with changes in, and that as a result identity thieves remain and will remain ahead of the regulatory curve for some time to come. A general conclusion from this discussion would be that legislation and company response is overly focused on the instrumental aspects of identity theft as a form of "theft" and that if a broader paradigm were to be introduced that calls the crime by its more accurate name, "identity fraud," comprising a host of other crimes involved with fraud that stem from an original theft of identity, this would refocus regulations from documents to individuals, from possession of documents to record of criminal behavior, and from reactive attempts to improve the security built into documentation and procedure, to a preventive approach focused on offenders. This more "cultural" approach to identity fraud may well have to derive from law enforcement, where a preventive paradigm has begun to inform crime fighting.

(vi) Analysis of Interviews with Investigators, Law Enforcement and Other Officials

In preparation for interviewing stakeholders in law enforcement, the criminal justice system and companies and organisations impacted by identity theft, the researcher conducted a review of the statistics regarding identity theft compiled by law enforcement.

(vii) Confounding Factors

It was in seeking to gain insight into the scope of identity theft from law enforcement statistics and other data, as well as from individuals in various levels of law enforcement and the criminal justice, that this research confronted its most formidable confounding factors. The

examination of law enforcement response consisted of two parts, an effort to gain a sense of the accuracy of law enforcement statistics on the incidence of identity theft, and interviews with stakeholders, from cops on the street, to investigators, to police officials, to criminal justice and company stakeholders, to determine the extent to which they acknowledged and were informed about the dimensions of identity theft as indicated by the research, and by both offender and victim appraisal of their work.

The first problem that emerged involved determining accurate statistics of incidence of identity theft, as might be compiled and published by the police department. The validity of statistics in reporting figures of crime have been subject to question for some time. A persistent lament in research is that the statistics published by organizations such as police forces rarely reflect actual events, threatening their validity (Skogan, 2003). According to Skogan's (2003) analysis, statistics in fact reflect the interaction between three sets of activities: things that occur in the environment (crime); things which are victimised by it (reporting), and society's effort to discover and record it (policing). That is, while crime occurs, whether or not all of crime is reported, and whether or not the police force has been diligent in discovering and recording the crime are all factors that contribute to the published statistic. It often happens, for example, that authorities, when discussing statistics, will hedge their conclusions by suggesting that the numbers really measure something innocuous like "acts which have come to the attention of the authorities" and constitute "socially recognized volume of crime" (Skogan, 2003). While statistical analysis often proceeds without consideration of these mediating factors, it remains that humans report crime and also record and classify crime, and each interaction in this process compromises the statistic and its validity.

The gold standard for crime statistics is the major statistical repository available to law enforcement, the Uniform Crime Reports (UCR), created in 1919. This database collects statistics from over 17,000 local and state law enforcement agencies in the United States. The statistics are then tabulated and the resulting raw data is disseminated to criminologists for them to assemble comprehensive crime data covering both crime rates and trends. Insofar as the UCR utilizes statistics from 95% of United States' police forces, as well as other factors, means that the statistical analysis and the relevant data derived from it are flawed. The gap between the statistic and the probable actual figure of crime that remains undiscovered in the community is termed in law enforcement the dark figure of crime.

Some jurisdictions are more motivated than others to adjust statistics to conform to the particular shape of the moment, given various political trends. For example, during an election year, crime rates become a political issue. Insofar as reporting of crime statistics is ultimately overseen by the executive branch, an executive seeking re-election might pressure departments to present statistics that do not highlight the fact that a crime rate is on the rise, as this might cost the executive re-election. There are numerous examples of stakeholder pressure being brought to bear upon statistical reporting, thereby distorting reporting.

Reporting behavior has been repeatedly questioned in the police department. Moreover, reporting problems have lead senior-level commanders to also bring a certain degree of apprehension to reported statistics, often causing them to dismiss, discourage interpretation or downgrade and minimize the importance of the reporting statistics. The New York City Police Department quite recently came under fire by individuals who accused the departmental hierarchy of 'fudging' crime statistics for various institutional or departmental reasons. Bennett, (2010); Ruderman, (2012) report that the NYPD claimed a major victory in reducing crime, as,

for example, homicides have been reduced by 20% since 2000. While it might be difficult to falsify murder statistics, as dead bodies in morgues cannot be argued away, past problems in NYPD crime statistic reporting have left a level of uncertainty by journalists and politicians as to the accuracy of the reported statistics each year. It was not apparent to this researcher that accurate statistics have been kept on the incidence of identity theft over the past ten to fifteen years. Identity theft, if a crime exists only if reported, must rely in particular on accurate and reliable reporting in order for the trends and figures to be adequately calculated. Due to the fact that it is an under reported crime, collected data is highly subjective and it varies depending upon the agency, resources, staffing and responses to the problem. Though the researcher shared some doubt in reviewing identity theft statistics from 2000 to 2010, even with a plus or minus margin of error, in the context of a policing environment which generally claims success in reducing overall crime rates, current NYPD statistics on identity theft indicate an increase of incidence of crime since 2000 by 750%. The comparatively high rate of identity theft is generally attributable to its status as a 'new crime,' meaning that law enforcement has not yet caught up with it, but also its higher rate in New York City can be explained by the fact that, due to the volume of money transactions carried in the financial capital of the world every day, the city has become a breeding ground for identity theft, making identity theft an alluring and highly profitable operation especially for organised crime groups. While engaging in distrust of reported figures, the stark profile of identity theft, alone among crimes undergoing dramatic rise over the past decade, is accepted as generally indicating the seriousness of the problem. An increase in globalisation trends has provided an abundance of identity thieves. An example of the transformation of identity theft and other crimes in the United States in specifically, New York City will be explored.

My findings for this work were based on my ethnographic observations of, and reflections on, the process of gaining access to the participants who were not readily available to the public for this study. The participants included, but were not limited to sources within the banking and credit card industry; individuals who are employed in the criminal justice system, namely, the courts, legislature, and correctional institutions; attorneys, ex-convicts, defendants, victims, family members, friends, academics, as well as individuals who are employed with the National Retail Federation. Additional findings were based on observations of participants who took part in a formal, panel discussion which was held at Utica College in New York State. The primary sources of identity theft data utilized in this research were generated from field observations at the Manhattan District Attorney's Office, Identity Theft and Cyber-Crimes Bureau, located in the Supreme and Criminal Courts building in lower Manhattan; The New York City Police Department's Identity Theft Unit, located at a training facility in Brooklyn; a United States Postal Facility, located in the Whitestone area of Queens; The United States Secret Service Office, located in Brooklyn, New York; New York City Police Departments, Manhattan South Grand Larceny Task-Force, located in the Midtown area of Manhattan. Additionally, law enforcement officials and attorneys from the Kings, Nassau, Westchester, Richmond County, along with Chicago's, Cook County District Attorney's Offices were interviewed. Officials from New York and New Jersey Attorney's Offices also provided information. Some assistant district attorneys at the Manhattan District Attorney's Office were forthcoming with information on the activities of identity thieves in settled cases. Despite explaining the information requested was public information, some attorneys were uncooperative.

Most of these interviews were partially compromised by confounding factors. There were several reasons why confounding factors had to be taken into consideration in compiling data from these respondents, more so from offenders or victims. It fairly frequently happened that I was unable to convince certain individuals to cooperate. Several prosecutors throughout the State of New York and Federal System, to whom I had been referred by friends, refused to give me the research information on identity theft. This was surprising because the statistical information I needed was considered public information, under 5 U.S.C. § 552. US Code. I also only required concrete information on cases that were already tried, plea bargained and disposed of.

A few examples of the difficulties encountered in gaining information or even interviews from various stakeholders are provided.

(viii) Reporter

This researcher reached out to a reporter because crime reporters are generally knowledgeable in their field. They have sources within and on the outside of organisations. I therefore realised it takes time for a reporter to cultivate their sources and understand the inner workings of the identity theft field. My initial experience in contacting a well-known crime reporter who is assigned to the press office at Police Headquarters was not met with enthusiasm. I explained to the reporter via telephone, that I was enrolled as a student at Cardiff University, Wales, U.K., and asked permission to speak to him and his colleagues at the press office about the identity theft articles that they cover. Surprisingly, the reporter put me on hold for a few minutes, returned to the phone and informed me that the research assignment that we discussed was impossible to carry out because no one was willing to spend the time conducting an

interview on the topic of identity theft. It is more likely that the reporter had developed a widespread network of contacts to write a story, and once these goals have been accomplished, the reporter is likely to protect his sources to ensure his credibility and confidentiality.

(ix) U.S Attorney's Office, Southern District

For one case, I was sent (by a friend and colleague in the legal profession who was assigned to the Manhattan District Attorney's Office) to the Southern District of New York to meet with an Assistant United States Attorney to gather pedigree information and related data on convicted individuals who had been sentenced for identity theft and related crimes. Even though I held law enforcement credentials and some national security clearance, I was put through a multi-step security check. The United States Attorney took me to a window-less conference room where we were joined by a supervising attorney who informed me their records were confidential and they could not divulge any information relating to closed cases in the U.S. Attorney's office despite the fact the information I sought was public information and I proposed to use it for educational research. One of the Attorneys cited Exemption 3, of the United States Freedom of information Act 5 U.S.C. 552 (B) (3) as amended by section 5 (B) of the Government in the Sunshine Act, P.L. 94-409, approved on September, 13, 1976, effective March 12, 1977. This Act stipulates that investigations by government agencies "be withheld from the public in such a manner as to leave no discretion, including all matters appearing before the grand jury." As a result, I was not allowed to examine any documents.

(x) **Secret Service**

As research proceeded to higher levels of work in identity theft, an increased perception of the changing nature of the crime as a 'new crime' emerged. A source at the New York office of the United States Secret Service is offered as typical of this response. He explained that "at one time in society you knew who the criminal was because he walked up to you or the bank teller and said, 'give me your money'." The source also explained that the police were able to address this kind of direct crime with minimal presence, and a good deal of what he characterised as good old-fashioned police work. The respondent then noted changes to this model over the past decade, "over the past decade, as offenders realised that there are lucrative opportunities in the identity theft market, we have experienced a proliferation of identity theft crime in the United States. Who needs a gun, a crowbar, a knife, a stone, a hammer, a lookout or a getaway vehicle to perpetrate a crime any more? Stealing identities has become the preferred modus operandi for the criminal".

(b) A New Dimension: Organized Crime

The link between the cop on the street and the farther reaches of identity theft would be the investigators in precincts or departments that specialise in identity theft. A series of interviews with special investigators with a focus on identity theft found that, at present, they appear to be caught between the local and global dimensions of this evolving crime. For one thing, street cops evinced some awareness of the larger ramifications of the crime of identity theft by voicing a frustration that most are asked by superiors to downgrade the crime by classifying it as a larceny. This is done to keep the statistics on identity theft down and presumably also to control precinct or department statistics on larceny. The problem with this

designation is that while it is true that the original act, such as a theft of a wallet, could be classified as larceny, larceny ends with the money being lifted from the wallet and the wallet disposed of, possibly to be found and returned to the owner, while for an identity fraudster the wallet is only the pretext, the beginning of the crime, and of a series of crimes that goes far beyond the wallet. Thus, the street cop is aware of this, and being forced for record-keeping reasons to classify identity theft as a larceny chafes against their awareness of the growing problem. With regard to investigators, their work very quickly takes them into the expanded dimensions of identity fraud, a process which involves the consumption of considerable investigation time and the generation of tremendous amounts of paperwork, which, counter productively, usually means, as they do not receive support staff, spending more time behind a computer screen filling out the paperwork, than out in the expanding field, seeking out the various tentacles of the identity fraud as it metastasises by organisation into greater crime.

There is also no central repository of data about identity theft, with investigators themselves reluctant to share data with ancillary units and other agencies. Insofar as investigators, as did street cops, reported that their superiors frequently intervene and try to dissuade victims from reporting the crime, ostensibly to falsely keep the crime statistics of the precinct down, also generally indicates that investigators must confront a police culture in which, become of the aforementioned disorientation or paradigm break, identity theft is often downplayed as a crime, and where the notion had taken hold that investigating identity theft is more trouble than it is worth, especially as investigation may not lead to any apprehension of the criminal.

The researcher also interviewed several prosecutors involved in identity theft cases in court. Many of these prosecutors felt that they represented the last line of defence against the

new and evolving crime of identity theft. Most reported that they were more or less satisfied with the legislative response to the crime of identity theft, believing that some laws had teeth which gave them a basis for more vigorous prosecution. At the same time, most believed that legislative response is slow and usually only happens, generally, after the fact, and after the identity theft crime has become entrenched in a new criminal way of life. Prosecutors generally believed that slow response to the crime of identity theft by legislation and law enforcement allowed it over the past ten years to become entrenched in the lifestyle of most criminals, allowing for, the eureka moments, perception of ease and lack of chance of detection or prosecution, which was routinely found in offender response to the crime.

Prosecutors directly faced the perception by offenders that their chance of prosecution and doing jail or prison time due to identity theft was slim. They acknowledged that current judicial response is weak, with limited punishment and light penalties. They acknowledged that there is a general impression in prosecution and in the courts that somehow identity theft is a victimless crime and that the court has better things to do with its time. They also expressed the notion that they perceived among their colleagues and the judicial and legal community generally an actual preference for identity theft over other crimes insofar as it was not a violent crime. They reported hearing prosecutors or defenders state on the record in court that their client, an identity thief, was not a bad person or a criminal, because there was no weapon involved in the crime, and no one actually got (physically) hurt. In contrast, the offenders clearly see identity theft as an extension of regular robbery or larceny. Those with criminal records are most likely to be involved in identity theft, as in organised crime, all offenders documented how they came to realise the potential of the crime. A process in which they “criminalized” activities which were previously overlooked, and then “weaponized” objects and utilities, i.e. computers,

forgery materials, that they had also previously overlooked: thus, the offenders became fully aware of the fact, as found in the research, that they are criminals, they live a criminal life, identity theft has victims, and they use “weapons”, only the weapons do not happen to be guns.

It may be said that identity thieves have shown that far from being innocent white collar criminals who are not ‘bad’ people. This researcher have interviewed individuals who as identity fraudsters today were violent offenders who now have found it advantageous to hide behind the veneer of non-violence and non-seriousness of identity theft crime. A further factor that prosecutors seem aware of contributing to this general perception of identity theft not being a serious crime is that, they perceive, there is little comprehension or awareness of the international scope of the crime, that is, how big small crimes can become. Only a handful of local prosecutor offices, in Manhattan, Southern District of NYC, for example, have even addressed this dimension of the crime, and even then lack the ability in terms of manpower to reach out from local to sanctuary jurisdictions where cyber-based fraudsters operate safely, in, for example, Eastern Europe and Russia, and any of the former Soviet Republics. Though now and then an investigation by a prosecutor will reach out into the global dimension of the crime, at present this is rare, what is required for an effective response to these enterprises is using local law enforcement personnel more effectively, by partnering them with investigators working out the dimensions of the fuller enterprise in Eastern Europe locales, for example. For all of this, it is apparent that prosecutors have developed a much more extensive awareness of the scope and scale of identity theft, and, for that reason, measured against the status quo, may experience more frustration than even the cop on the street with regard to current response.

Almost all prosecutors interviewed universally adopted a punitive approach to discussion of a solution. They felt that what was needed to stem the rising tide of identity theft was more

consequence. That is, the criminal prosecution system needs to respond directly to the generally acknowledged perception by offenders that there is little chance of being prosecuted for the crime, and, if prosecuted, sentences are comparatively light, and therefore, no problem. To respond, prosecutors believed the jail time for identity theft needs to be made harsher, the financial penalties for identity theft much more onerous, and the consistency and diligence of prosecution response much more regular. That is, insofar as identity thieves currently view the crime as easy, with great rewards, and light sentences and limited potential of arrest, all of these criminal justice system contributions to the weak guardianship aspect of the routine activities theory formulation of the crime need to be addressed. At present, prosecutors were so firm in their conviction that the consequences and penalties against identity theft need to be increased, as a first step in response to the crime, that no discussion was entertained as to whether or not simply adding more punishment, as opposed to engaging in preventive measures, on the consumer side, was the better approach to stemming identity theft.

(i) Russian Organized Crime Case

From a study of records and interviews with stakeholders the facts of an important case of identity fraud were derived, developing a much fuller sense of the extent and seriousness of Internet-based identity fraud than previously acknowledged by other stakeholders. On August 16 2007, the Manhattan District Attorney, Robert Morgenthau, announced the indictment of five men on charges of participating in an identity theft ring while $1.5 million from wealthy Americans. Additional attempts were made by the group to steal up to $10.7 million from other accounts. Four of the five men had already been arrested, and were being held in other states. The arrest was made when the leader of the ring, Igor Klopov, a 24 year-old Russian, was lured to New York through a sting that informed him that he had to collect $7 million in gold which

had been purchased with money stolen from one of his victims by an associate. Klopov was an expert in mining the Internet to obtain personal information about potential victims. He would target home equity lines of credit (HELOC) held by wealthy persons who owned expensive property, found through the Fortune 400 list of wealthy persons, such as Silicon Alley victims, a Texas business man who headed a major credit card reporting agency. Most of his victims were in California and Texas, where ownership deeds are available online. Klopov had many aliases online and only communicated with associated through email or instant messaging, making it difficult to trace him.

Needless to say, Klopov's operation represented identity theft on a new, grand scale. To better understand record keeping routines that enabled his practice, it was necessary to gain insight from a specialist in real estate law, with the intention of determining how common the reporting of real estate sales online might be. On February 27, 2012, an interview was conducted with James McCutcheon Esq., a real estate attorney of the law offices of Arthur and Associates, PLLC, New York City. McCutcheon explained that there is a comparable system, the Automated City Register Information System (ACIS), in New York, to the ones exploited by Klopov in Texas and California. This database is also readily available to the public. An individual may enter a street address and find all the information he or she needs regarding ownership, including the length of time owned, the chain of ownership, and even obtain a copy of a deed. This strikes one as a routine activity by the City of New York that, it is now apparent from Klopov's discovery, enables high-level Internet identity theft, and which was specifically exploited by Klopov.

Klopov was apprehended by an uncover investigation. This involved an undercover

investigator from the Manhattan District Attorney's Identity Theft Squad infiltrating his Internet operation by leading Klopov to believe that he was willing to engage in illegal activities online, and ones that would further Klopov's scheme. This investigation, revealed in discussion with the investigator, found still another twist in Klopov's identity theft schemes. He obtained personal identity information by trolling the Internet, but, then, kept a dossier of background research on his targeted victims, and even hired private investigators to obtain more information on the target. This too was a strategy, affordable perhaps only by high-level identity fraud organizations, that was new to the crime profile of identity theft.

In addition, Klopov further exploited the Internet in novel ways to expand his operation. He recruited accomplices from the on-line job hunting sites Monster.com and CareerBuilder.com. He then would provide recruits who agreed to participate in his scheme, such as Lee Monopoli, with fake identification documents, back dossiers on identity theft victims, make all their travel arrangements, and even provide them with five-star hotel reservations, limousine services, and travel expenses, all paid for by stolen credit card numbers, still another extension of the purchasing of stolen goods dimension of Internet-based identity fraud.

Klopov also hired experts in particular forms of identity theft, bringing all counterfeiting and other operations within his empire. Wesley Watson was hired by Klopov to create high-quality counterfeit identification documents for new recruits, and also forged for the new recruits all the documents they would need to steal funds from the victims' financial institutions. These documents included powers of attorney and transfer request forms, used to transfer stolen funds to accounts held by other conspirators. Another conspirator, James Dalton, was hired by Klopov to receive and distributed unauthorized checks and other items in connection with fraudulent account withdrawals. An example of the kind of fraud operation enabled by these documents,

the case of theft of funds from Fidelity Investments is enlightening. In 2005, Klopov requested from Fidelity Investments the sale of $1 million in stock held by his victims, a couple in Silicon Valley. The act was expedited by having one of his recruits appear at the Fidelity Investment office in San Jose, California, with a counterfeit power of attorney said to be signed by the couple. Five days later, the $1 million was wired from the couple's account to an account at Washington Mutual Bank in the name of one of Klopov's co-conspirators. Later in the day, Klopov had the $1 million wire transferred to bank accounts in Russia, beyond the reach of Western police.

A few incidents in Klopov's career indicated that, now and then, red flag rules lead to the prevention of a scam. In one scam, in 2006, Klopov gave one of his recruits the personal identification information of a wholesale food broker in Dallas, Texas. The recruit was flown to New York and provided with counterfeit identification superimposed upon by a photo of him, then asked to go to a branch of Washington Mutual Bank in the East Village to withdraw $220,000 from the victim's account. However, in this case, the bank manager became suspicious, and refused to allow the transaction to go through. In a second scam, Klopov attempted to steal $620,000 from a Merrill Lynch account held by a resident in Oregon. The recruit was provided with a copy of the victim's signature, a fake driver's license with the victim's personal information on it, and a photograph of the recruit on it. Watson prepared the counterfeit documents such as power of attorney and also documents which requested the transfer. This wire transfer request, with documentation, was wired to Merrill Lynch in New Jersey. Fortunately, security officials at Merrill Lynch, working with detectives, detected the fraud and prevented the transaction from going through. In a third case, Klopov had Watson create false documents for still another stolen identity, the president of Trans Union Credit. Monopoli was

the recruit who then went to a Manhattan branch of J.P. Morgan Chase Bank with false documents to request information on accounts. Bank employees, cooperating with the police, became suspicious, and blocked the withdrawal.

Klopov's operation also necessitated a way to launder money. He did this by stealing the money, then purchasing gold. In November 2006, Klopov began manoeuvring to steal $7 million from Charles Wyly Jr., contacting J.P. Morgan Chase, posing as Wyly, requesting a new checkbook be sent to a Texas address, of a Klopov conspirator, the checkbook, which was linked to a HELOC account, was sent, the conspirator then sent the checkbook to Watson, who drafted a check from Wyly's account for $7 million, then sent it to a gold dealer in Westchester County, New York. The gold dealer, however, though to verify the check, so called its bank. Unfortunately for Klopov, the bank was also J.P. Morgan Chase, which then contacted the real Wyly directly, who informed the bank that he did not sign a $7 million check to purchase gold. It was this case that lead to Klopov's arrest. J.P. Morgan Chase's security personnel notified the Manhattan District Attorney's Identity Theft Unit, the detective squad as well as the Secret Service. At this point, the decision to arrest Klopov was made. The modus operandi was in keeping with Klopov's reality. The undercover officer working with Klopov called him to inform him that the money had successfully been used to purchase gold, which the undercover detective proved by having a picture taken of him standing next to the gold, and emailed to Klopov. The undercover detective then made arrangements for Klopov to travel to the United States to retrieve the gold. Klopov balked, but agreed to travel to the Dominican Republic, where he nonetheless was met by U.S. Secret Service and NYPD investigators from the District Attorney's Squad, all working undercover. Klopov developed trust in his hosts and acquiesced to their explanation that he would still have to travel the U.S. to collect the gold. He entered the United

States, believing that he was entering illegally, in May, 2007, and immediately arrested. Klopov was charged with conspiracy, grand larceny, money laundering, forgery, criminal possession of a forged document, criminal possession of stolen property, criminal possession of forged devices and identity theft.

These scenarios indicate a level of complexity in identity fraud unsuspected by most offenders and, of course, victims, but also a large part of law enforcement officials as well. In addition, these incidents indicate that, when banks are involved, red flag rules and breach notification does, now and then, work to prevent a crime being committed. It is also true that it was by means of a red flag that the path to arrest was begun. Finally, the case also demonstrates the high level of involvement of specialist investigators in identity theft, and their willingness, in cooperation with the Secret Service, to venture into the global web around which Internet-based identity fraud is expanding. The scope of this theft scheme, indicates even Klopov's lack of ultimate sophistication (which would entail making all thefts entirely electronically) was that he employed recruits who went to banks in person, and made illegal transactions in person, a fact which localised the crimes and allowed for undercover police to infiltrate the network.

For all of this, Klopov was sentenced by the judge to the maximum fine applicable to the offenses at the time of sentencing, and he received—three to six years in state prison. Some of his conspirators were also convicted to the same time. After the defendants were sentenced, I asked for, and was granted permission to interview one of the sentenced inmates just before he was transferred to state prison. Unsurprisingly, given the millions that he had been involved in stealing, the identity theft viewed a three to six year stay in prison as a vacation from his routine worries, which he could use productively to plan new operations upon his release. He also

boasted that the stash of money he had gained was safe in offshore accounts, waiting for him upon his release.

(ii) Zeus and the Money Mules

Soon after, NYPD detectives became aware of a new way for identities to be stolen, Zeus Trojan. A case involving a identity fraud ring making use of Zeus Trojan first came to light when the NYPD detectives visited a bank in New York City to investigate a suspicious $24,000 withdrawal (meaning that, again, a red flag rule functioned well, and that the physical site of the detection was viewed as the 'crime scene'). Upon investigation it was found that the account had been subjected to a cyber attack from Eastern Europe making use of Zeus Trojan, a malware which is attached to benign e-mails sent to small business in the U.S., embeds itself in computers if the email is opened, and from that point on records keystrokes of account numbers, passwords and other security codes logged onto bank accounts online. This information is then used by hackers to take over the victims' bank accounts and transfer all money in the account, thousands of dollars at a time, to receiving accounts controlled by the thieves. The receiving accounts were set up by a 'money mule organization" consisting of individuals who had entered the U.S. on student visas, fake foreign passports and with the goal of opening up false-name accounts at U.S. banks, to which the stolen money would be transferred. Once the money was transferred from the stolen account to the fake account, the money mules were then instructed to further transfer the proceeds to other accounts overseas in Russia and Moldova, or to withdraw the money and smuggle it abroad. The discovery of these schemes launched an investigation conducted by the Manhattan District Attorney's Office, the NYPD, the FBI, and the United States Attorney General's Office in New York City, the Department of State Diplomatic Security Service and the

United States Secret Service. It culminated in the arrest of 20 individuals, most of them Russian nationals.

Sofia, who had opened a false account at Chase Bank, received $14,500 in wired money, and withdrew $12, 000, was apprehended at a New York airport with a false passport under the name of a Yugoslavian national. Another mule was arrested at a bank in New York City while attempting to open a new false account (he was arrested, arraigned, released on bail, and opened another false account four days later). Most of the other arrests were of mules that all opened between two to eight false accounts, and had trafficked in the area of $20-80, 000 overseas. All also worked under false passports. All were indicted for conspiracy to commit bank fraud as well as conspiracy to possess illegal passports. All were associated with hackers and individuals abroad who provided them with fake passports, but none of the overseas part of the network was dismantled. The indictments indicated that several members of the mule organization had also tried to breach brokerage accounts at E Trade and TD Ameritrade, Inc. more or less by the same means, transferring money to shell accounts, from which, in turn, the money was transferred overseas. These transfers were more substantial, amounting to $1.2 million, and more international, much of the money transferred to accounts in Asia. Some of the funds, however, were also withdrawn at ATMs in New York City.

This mule organisation made use of a highly sophisticated internet hacking instrument to gain access to accounts, but then was forced to circumvent red flag rules, which would have alerted account holders to large transferrals overseas. By sending mules to New York City, the crime was achieved with false identities to open up fraudulent accounts in U.S. banks, from which a transfer to Eastern Europe would not arouse suspicion, or withdraw it in person. This same scam was used for Etrade accounts. However, it was a suspicious transfer that alerted a

bank employee, who called the police. Also, one mule was arrested while trying to open a fraudulent account in person at a New York City bank. Finally, each mule was a small piece of a large puzzle and on average did not transfer what would be considered large amounts of money. It is not likely that any mules knew very much about the organisations they worked for. None of the overseas hackers or organizers who profited much more handsomely from these transfers was touched. In this case, the complexity of the organisation was made vulnerable by the bricks-and-mortar nature of the mule operation, devised to circumvent red flags. Even so, while NYPD was able to arrest the mules, a gap remained between their access to the identity thieves, and the real thieves profiting invisibly online overseas. This case, then, largely extracted from examination of case files, with commentary by investigators involved in the case, again highlighted an organisational complexity in identity fraud that far exceeds the understanding of individual mules arrested by law enforcement—a fact that at present dramatizes the gap between law enforcement and the scope of the crime.

(iii) A Multi-national Ring

In the summer of 2009, an individual was debriefed as a part of a joint effort between the New York City Police Department Identity Theft Unit, a confidential unit within the Department of Homeland Security, the United States Secret Service and the Manhattan District Attorney's Office Identity Theft and Cyber Crimes Unit. The researcher was privy to details of the debriefing, through confidential sources. The results of the debriefing provided evidence of a large-scale, currently operating crime ring of identity thieves making use of forged credit cards for the purchase and selling of Apple products on the international black market. The investigation determined that the ring had been in operation for about two years. The ringleader, running his operation from jail, where he was already serving time for an earlier identity theft

scam, recruited individuals who worked in the service industry to steal customers' personal information which was then sold to organized crime groups in the Middle East, Europe, West Africa and Asia. Crime bosses in countries in other parts of the world, including Libya, Lebanon, Nigeria, Russia and China hired 'skimmers' who used high-tech equipment to steal credit card data from victims, then download the data onto magnetic strips of blank plastic which resembled credit cards. Some credit cards and state driver's licenses were forged using printing machines. The bogus credit cards were then used to finance an estimated $13 million nationwide shopping spree in the U.S. focused on Apple products. The bulk of these stolen goods were then packed into containers and shipped globally to the worldwide crime bosses.

As a result of this ring, known in confidential circles as "Operation Swiper," 180 individuals associated with five crime enterprises operating out of Queens, New York City have been arrested and charged with identity theft. The investigation is ongoing. While this operation structurally resembles the Russian operation, wherein a crime boss overseas managing his recruits state side, the fact that the recruits were U.S. nationals or immigrants working in the service industry combines identity theft and employer theft at a new scale. The fact that the stolen data was sent overseas to be converted there into credit cards which were then processed back in the U.S. to target fraudulent purchase theft of, specifically, highly desirable Apple products also represents a twist away from site-oriented crime. At the same time, the recruits still were in the U.S., and still had to engage in criminal activity, in terms of forgery and fraud, in the context of organized crime, to make them accessible to law enforcement. Nonetheless, while arrests were made, demonstrating what can be done if NYPD works with more globally-focused agencies, the case study represents still another example, derived from confidential investigation

into the case, of the ever-expanding global dimension and ever-creative twists and turns involved in tracking and stopping large scale, organized-crime based identity fraud.

All of the facts of these cases or operations were gained from insiders in law enforcement investigating identity theft. That is, while gaining general information on the street-level crime of identity theft was difficult and often confounded, and in general it was found that statistics on identity theft at this level were downplayed, it is also true that more specialized higher-level law enforcement officials have launched investigations which have served to reveal still more complexity and scope in identity theft, beyond even information about organised crime involvement gleaned from offenders. Moreover, when identity theft escalates to identity fraud carried out on a mass scale in a globalised theatre it is no longer difficult to gain the attention to the crime from higher-level officials. Though this attention may be due to historical concerns regarding organised crime, and that identity theft has become a new vehicle for the revitalisation and spread of organised crime, this nonetheless represents one area where law enforcement has exceeded research, government legislative response and even individual offender awareness, to explore the outer limits of identity fraud today. While it remains true that at the level of the cop on the street law enforcement continues to struggle to find a framework of response which will be perceived as effective by offenders and victims, and that criminal justice needs to toughen penalties for identity theft in order to back up this effort, and that from this perspective the escalation of identity theft into wholesale identity fraud gives the crime the character of a 'new crime' trend that is out of control, once it does escalate entirely into an organised crime operation law enforcement has a historically proven apparatus of response derivable from previous campaigns against organised crime, whether through RICCO laws or other means, to address the crime, and at this level it can and has taken action. It therefore would be a false conclusion to

agree with offender and victim alike that law enforcement is helpless and ineffective against identity theft; the correct conclusion is that law enforcement has tools of effective response at its disposal to combat identity fraud. What is required is that the identity theft response be conceptually aligned with the response its organised crime dimension, a process which may bring cop on the street response in line with the expanded response to the widest dimensions of the crime today.

Applying the situational crime prevention paradigm and routine activities theory to these crimes is more difficult, but weak points in routine practice are evident. For example, while in several cases red flags and breach notification procedures were effective to stopping the crime from occurring, the ease with which accounts were accessed remains a problem. The offender must be identified as the ringleader, and his motivation remains high because he can perform his theft through the proxy of low-level recruits or mules. In terms of suitability of target, it is not apparent what seasoned and experienced financial persons of wealth could do to better protect their accounts from hacking: that is, this matter is an organisational and banking issue. Therefore, for these crimes, the bulk of the responsibility lies on the shoulders of the guardianship and the need to strengthen this side of the equation. Weak spots identified in these cases were the ease with which one, even a fraudster, can open a new account, without further identity check or other safeguards. It is also surprising the ease with which one, even a fraudster, can withdraw large amounts of cash or make large scale transactions to foreign bank accounts without further security clearances or alerts being written into these institutional routines. While it is true that proposal of any further constraints for the purposes of security might be protested by banks and citizens as an infringement of civil rights, this issue must be addressed: organised crime at

present seems to identify weaknesses in the current banking system both off- and online and exploits them.

(iv) Summary of Interviews

The data analysis for this part of the study was comparative, that is, involving comparing the perceptions of respondents in interviews to questions about the nature and extent of identity theft, and then, in order to determine if their knowledge was limited or extensive, the degree to which their answers compared to the current level of knowledge about identity theft as indicated by a baseline measure of data discovered in the review of literature. A simple comparative benchmark was established for the level of knowledge of each group of respondents, less than, about equal to or extending beyond the findings of the current research. It was hypothesized, given the researcher's experience, that the knowledge of most respondents will be limited and fall short of best practice. This hypothesis was confirmed as, in response to the research questions as they apply to this chapter, as in responding to, What is identity theft?, while the research has begun to adapt a routine activities theory framework and thus gain a sense of dynamics of the crime in everyday circumstances involving trash, banks, ATMs and other sites, it continues to struggle to gain a full sense of the extent of identity theft crime on the internet. By comparison, investigators by and large seemed focused on street-level, bank-locational, community-oriented identity theft crime, likely due to jurisdictional issues, and have little sense that they should be or even can be involved in combating internet-based identity theft. Even more limited is the perception of the relevance and importance, the nature and scope of identity theft in police officials, whose management style is understandably focused on street-and community-level crime, especially being aware of internet-based identity theft in the abstract, as something for federal officials to account for.

With regard to research question two as it relates to the research versus the interviews of investigator and officials, How did identity theft evolve as technology and cyberspace became readily available to the general public?, as noted, research struggles with this question, and both investigators and officials are behind the curve in terms of keeping up on the degree to which technology is greatly increasing offender motivation to enter this field of crime. With regard to question three, Who are the identity thieves, what methods do they use in committing identity theft and how did they acquire the skills that are needed to commit identity theft?, the research evinces a limited conceptualisation of these issues (compared to data extracted from actual offenders, see below), and investigators and officials continue to harbour traditional criminal profile conceptualisations of possible identity thieves, when, here too, the current level of motivation and opportunity provided by this kind of crime has brought in many more types of persons into identity theft than generally perceived. With regard to research question four, Who are the victims of identity theft, how do they expose themselves to the identity theft and how has identity theft altered their activities and behavior?, the same gap emerges.

It was hypothesized that, due to the focus of law enforcement, investigators would have a greater knowledge of the nature and extent of identity theft at present, compared with officials, but that both, due to elements of police culture, might still have conceptualisations of the nature and extent of identity theft that falls short of current reality. It was therefore hypothesized that the guardianship required to prevent identity theft is in absence or inadequate, with the law enforcement in particular challenged by the threats of online identity theft. This hypothesis was supported at the precinct or department level, but not supported in more specialised investigative response to identity theft.

(v) Summary of Findings

The findings of this study were determined by research in the literature and in the legislative documentation and police records regarding the prevalence of identity theft, and efforts being made to combat it. The primary source of data, however, was a series of interviews with three groups of stakeholders. These included, first, fellow investigators specialising in identity theft, police officials and stakeholders in other impacted areas of the identity theft crime dynamic, such as officials at credit card companies; offenders; and victims.

With regard to other stakeholders, who have a stake in reducing credit card fraud, credit card companies were hesitant to discuss the proliferation of identity fraud. That said most expressed frustration that identity fraud had been allowed to become such a major problem for their industry, suggesting that they blamed law enforcement for its slow uptake of prosecution of the crime. Those credit card officials interviewed were aware of the fact that the number of consumers experiencing credit card-based identity theft was on the rise, but most still expressed the notion that it would not be cost effective to put into place any company-originating defence mechanisms to combat the problem. That is, at present, most credit card officials saw credit card theft as part of the cost of doing business, not yet of sufficient volume that it demanded a systematic response. With regard to the invention of a chip that, if placed on credit cards, would do a great deal to hinder the crime, most officials acknowledged that they knew of the chip, but all, at present, believed that the prospect of installing the chip in all credit cards currently in the consumer marketplace would be too costly. The fact that most credit cards companies continue to rely on insurance companies to cover the costs of losses due to credit card fraud meant that at present most officials were content with the status quo. Again, this evinced a cost of doing business attitude toward credit card-based identity theft. Thus, for the most part, credit card

companies expressed the thought, though with a bit more tact, that at present they continue to make a tremendous amount of money in the highly lucrative credit card business, and that as long as identity theft does not cut into profits at any substantial level, they are not motivated to alter the current regulatory protection paradigm, which primarily involved reimbursement of the consumer and insurance companies covering their loss. The bottom line that appeared to emerge from interviews with credit card company officials was that as long as the credit card business remains robustly profitable, any serious attempt, originating with them, beyond the Red Flag rule paradigm, will not be emerging.

With regard to the views of police officers, investigators and officials who were interviewed with regard to identity theft, a variety of viewpoints were expressed. The cop on the street, that is, active duty police officers responding to calls by victims concerning identity theft, reported a varied intensity of identity theft as part of their daily beat. While some reported only rarely encountering identity theft, others were more alert to the fact, likely due to their different precincts and their demographics, that identity theft has rather recently increased to the level that they are aware of it, and aware that it is growing fast, and has grown fast, over a very short period of time. In both cases, however, the cop on the street expressed bewilderment over the nature of the crime of identity theft which indicates the extent to which this crime breaks the paradigm by which most on-the-street level crime is addressed. Most saw identity theft as an entirely new kind of crime, because when they responded to a call over identity theft and arrived at the "scene of the crime" there was no criminal, and no physical scene. They could not chase the identity theft criminal through alleyways or over rooftops and physically apprehend them, and take them away in handcuffs, apprehended. The identity thief was not near the scene, they were a shadow. Since the crime as reported by a consumer victim, for example, in paperwork

provided by a bank record of recent activity in an account indicated, the identity theft, while coming to the awareness of the victim at a bank located in their precinct, was also likely to have taken place overseas, leaving the cop on the street to only respond that, because of the extra-jurisdictional nature of the crime, there was nothing they could do about it. Everything about this crime was on paper (even there, there remains considerable uncertainty as to the role of official police reports in identity theft crime, with banks often absorbing a report of a loss made by a security company hired for them as proof of crime, and reimbursing the victim in house, without reference to the police). The fact that most identity theft victims did not even becomes aware of the crime until sometime after the crime had taken place, or until the next time they checked their banking account activity record or balance, further distanced the crime from the usual turf-based procedures of police crime prevention. Many police officers responding to complaints of identity theft, except in cases where wallet thefts were reported (but fewer ID thief's work in this way), also reported, therefore, feeling somewhat helpless, their public profile compromised by the fact that they can in no way demonstrate their control of the situation through an apprehension, high speed pursuit and other activity identified by the public as part of a police presence.

The general findings from these interviews are as follows: Police response to identity theft, viewed from the bottom up, that is, from the cop on the street, is inadequate, as most street-level officers and precinct commanders are assigned to focus on site-specific crime in their precincts, and often dismiss identity theft as not occurring in their jurisdiction. Thus, the rank and file of NYPD undertakes a response to identity theft and fraud that must be characterised as far from best practice. The fact that statistics on identity theft indicate substantial growth in the crime, and yet no serious effort to reformulate a framework for addressing this crime has been

developed at precinct level, indicates that commanders are pressured to deliver crime reduction statistics in key politically-sensitive crimes and must focus their efforts on them. The fact that police culture tends to identify protection with prevention of violent crime, including armed robbery, assault, rape and murder, would also lead commanders to minimize identity theft as a crime. At the same time, while the overall picture gained of the NYPD as a whole is far from best practice, at the level of special investigation in cooperation with detectives from federal agencies, some progress is being made in gaining a fuller perspective on the scale and scope of identity theft as it has evolved, through the involvement of global organised crime, into identity fraud mutating constantly into many different forms and scams. Case studies presented as an indication of this indicate a growing awareness of the new dimensions of the crime, and the capability of law enforcement, supported by mandates originally designed to combat organised crime, such as anti-conspiracy RICCO statutes, to address these crimes, and make large-scale arrests. That said, after the arrest, the length of sentence remains inadequate as deterrence against these crimes and currently is by no means a deterrent to the spread of ever more complex scams.

It is clear from these responses that the typical profile of a report and response to a crime must change in the case of identity theft. It is certain that the originating incidents of identity theft continue to happen often in the real world. Offender testimony indicated that at the origin of much identity theft is ATM-based theft, shoulder surfing at ATMs or supermarkets, exploitation of clientèle at bars or nightclubs, exploitation of guests at hotels, including dumpster diving, robbery of houses, etc. In all cases, however, if the offender leaves no trace of the theft, because, for example, they were less interested in stealing physical consumables at a house than lifting data, it is unlikely that a call will come in reporting a crime until much later when the

victims finally realise what has been stolen from them. While it is possible that a victim will be able to identify with suspicion the locale where he or she believed his or her identity was stolen, the fact that the restaurant, bar, bank or other sites is not culpable, unless compromised employees are identified, again problematizes police response. Nonetheless, it does appear that the cop on the street can work to conform identity theft to other robbery or larceny in the physical world by making preventive visits to all locales in the precincts which transact business using consumer personal information and perhaps even respond to identity theft crime at the location where the victim suspects the crime was committed. On the low end of the identity theft crime spectrum, then, there is some room for reducing current disorientation of response by police; at the high end, that is, after the ID has been sold and converted into other IDs and other crimes committed, the fact that illegal purchase of goods is likely to take place out of precinct or jurisdiction, or even overseas, still makes it possible, under current law, for the police to response.

Two points derive from this analysis. It is apparent that while identity theft organised crime rings have developed chains of crime that lead from precinct out of jurisdiction even overseas, and have thereby expanded the dimension of identity theft crime exponentially, law enforcement at present is only beginning to respond by the creation of a similar smooth continuum between jurisdictions both in terms of dissemination of information and the degree to which the local cop can become involved in reporting and pursuing identity theft crime that spins out from precinct to the world. In this regard, law enforcement is behind organised crime in identity theft. At the same time, law enforcement has demonstrated, with the response of police involvement to the call for it to become more involved in the War on Terror after 9/11 that it has the ability and capacity to expand the boundaries of the precinct to the world, and create a new paradigm according to which the local cop is much more aware that in addition to responding to

a local crime he may also be responding to a crime that has international implications. Therefore, this is a form of response that can be done, so that, when the local cop at the local precinct looks at a police report filed on identity theft which was only made aware to the victim when they checked their checking account total at the local bank in the precinct, they will not say, there is nothing I can do, but they will know what to do, and how to respond. This conclusion, then, leads to a broader level of law enforcement involvement with identity theft, and it is at this level that police response appears to be producing some positive results.

(c) Conclusion

Overall, then, the varied response of the cop on the street, investigators specialising in identity theft, officials linked to credit card companies, and prosecutors in the criminal justice system and courts, nonetheless point to some general conclusions. First, combating identity theft effectively will demand a change of paradigm and a change of culture with regard to how the crime of identity theft is perceived. Identity theft is not a form of larceny, but a new kind of crime, which demands new kinds of responses. Identity theft is not a victimless crime, as espoused by prosecutors fixated on violence as the primary measure of the seriousness of crime. Identity theft is not a small or insignificant crime, not worth the effort, in terms of investigation, to solve. Identity theft is, rather, a growing problem expanding exponentially in chains of criminality to global dimensions causing serious financial distress to myriads of victims in dollar amounts escalating to ever higher levels of seriousness. The paradigm of identity theft must be realigned with the example of high-level wide scale cases of organised crime placing the potential that all even minor identity thieves will be working for much larger organisations as the

norm. With the amounts now being pilfered in wholesale fashion from accounts and industries, it is no longer possible to view identity theft as a minor crime. Insofar as identity theft is perceived as easy to do, with great rewards, and little fear of arrest or prosecution, identity theft has also been allowed to become entrenched in criminal life, in gang life, in organised crime life, and thus is quickly in the process of becoming the primary criminogenic reality of criminal life in the coming years (much, as, for example, alcohol became the basis for the quick development of organised crime during prohibition during the 1920s).

As to be expected, the overall response of persons connected with law enforcement or criminal prosecution generally argue that deterrence must be increased in order to stem the spread of the crime based on criminal perception of the ideal combination of ease, reward and few consequences. This first response will mandate creation of still stronger laws, in a timelier manner, consisting of stiffer penalties for identity theft, including harsher, longer prison terms, and more onerous financial penalties. On a broader level, investigators in particular argued that in order for criminal prosecution to change its culture and become truly aware of the dimension of identity theft technology needs to be advanced to the state where a central database of identity theft exists, and means exist to track crime chains globally. This database, on the model of CompStat, for example, needs to offer full access to the cop on the street as well as high-ranking officials. On the preventive side, technology, both on the Internet and at sites such as ATMs, needs to be improved, to prevent identity theft. Police also need to engage in proactive policing tactics in terms of better educating the public so that their routine activities do not leave them vulnerable to identity theft. Therefore, according to the routine activities theory, offender motivation for identity theft needs to be reduced, target suitability needs to be reduced, and presence of guardianship, in this case both direct and indirect, needs to be enhanced. The entire

current imbalanced equation provided by routine activities theory as its formulation of the dynamics of criminogenic scenes needs a complete readjustment away from the current state favouring the offender to one in which the victim is informed and empowered in way that greatly reduces the likelihood of the continued growth of this new kind of crime.

CHAPTER 7: Conclusion

(a) Conclusion and Summary of the Research Findings

This study has explored the dynamics of the current situation involving identity theft both in offline and online contexts. The study argued, broadly, that the current approaches to identity theft prevention or detection, introduced by legislation and corporate governance, and consisting of red flag rules, breach notification laws and acquiescence to those regulatory measures by law enforcement, have not been effective in reducing identity theft. Indeed, so far have they failed, identity theft has grown exponentially in the past decade, and at present most identity thieves act with impunity and no fear of prosecution, a fact which caused identity theft to become almost viral and epidemic in nature, pulling in all kinds of criminals into this type of criminality. These dynamics have all but made identity theft comparable to bootlegging during Prohibition in the 1920s, the crime of the first decade of the 21st century, in terms of contributing to the expanding criminality of society in general.

Because of the failure of the current paradigm, this study proposed that it is time for law enforcement to begin to take identity theft more seriously. Law enforcement can make a great contribution to the combating of identity theft by drawing upon a key criminological theory that would fully explain the dynamics of the identity theft situation, and offer the empirical basis for a more holistic response to the crime, whether offline or online. The situational crime prevention paradigm, and, in particular, routine activities theory, based on rational choice theory, or the notion that criminals make cost-benefit calculations before a crime, and base that calculus of opportunity on the dynamics of a particular crime situation, strikes one as an ideal model to apply to identity theft. Some research (Haywood, 2007; Wortley & Mazerole, 2008) has already

shown the potential of the routine activities theory approach to preventing identity theft in limited situations. Routine activities theory argues that a crime is created by the opportunity offered by a particular situation, and its dynamics, measured by three main factors, offender motivation, suitability of target and absence or presence of guardianship. This study chose to apply this theory to identity theft by interviewing stakeholders representing these three elements in the identity theft situation, that is, stakeholders in law enforcement, identity theft offenders, identity theft victims and criminal justice and other regulatory entities connected with identity theft to gain their perceptions as to the criminogenic opportunity that currently propels this type of crime. On the basis of a data analysis of the responses of these three groups of stakeholders, an appraisal was made of the overall opportunity structure of identity theft situations at present, and whether or not these situations could be characterised as criminogenic or preventive of crime. On the basis of this appraisal, recommendations were made as to how to best combat identity theft.

Offender responses indicated that at present they are highly motivated to participate in identity theft. At the same time, most of the offenders interviewed reported currently engaging in very simple forms of identity theft, and the broader potential of the crime, especially the horizon of involvement of organised crime and gangs, is less apparent to them. Many of them had to learn on the job from others how best to exploit the identity data they had stolen; some did not even know what to do with a stolen credit card, though they understood that it offered them an opportunity for crime. The current situation, at the time of the interviews, then, indicated that we may be at a critical turning point where criminals in all walks of life are on the verge of coming to fully understand the potential of identity theft, and that this may be developing as a simple individual thief model evolves into organised crime and gang-related efforts which allow for

counterfeiting, maxing out of credit card accounts utilized by numerous persons at once, trafficking goods stolen with stolen personal data overseas, the increased globalization of the crime, and obtaining all manner of illegal documents based on stolen personal data to set up fraudulent lifestyles for criminals or illegal aliens. That is, we may be at a turning point in identity theft. Though not all interviewed offenders were fully aware of this, it might be a matter for further research to study the level of offender awareness of the criminal potential of identity theft in five years. Offenders universally agreed, however, once they got into the crime, that identity theft, for them, was the perfect crime, relatively simple to pull off, with a high pay-off, and very little chance of apprehension, and, if apprehended, comparatively light sentences, if any. Most offenders acted therefore with impunity in identity theft, believing that law enforcement at present was helpless to deter their new favoured crime. Therefore, with some more detailed qualifications, this study concluded that, in terms of the offender motivation factor of the routine activities theory equation of criminal opportunity, current offender motivation for identity theft is high, and expected to remain high for the foreseeable future.

With regard to victims, the study found that high offender motivation was matched as high target suitability. Several factors contributed to this. For one thing, most victims had little or only dawning awareness of the dimensions of identity theft, and therefore had not yet absorbed the need to take precautionary measures to prevent the crime from happening to them. While the crime having happened to them clearly changed their behavior, most victims interviewed would have to be classified as “sitting ducks” in the sense that they behaved in what is generally accepted to be highly loose ways with their personal data. Though in some cases the viral nature of identity theft raised its head in such as way as identity theft could not have been predicted, and it is unlikely that a preventive measure would even have been conceptualized (old

mail delivered to an old address by the USPS resulting in the new occupant opening it and stealing the personal data), it is also true that a number of victims, especially online, responding naively to phishing or email fraud schemes, causing their personal data to be stolen. While it was found that if the theft occurred in a physical format or in a specific locale like a bank, redress was quick, and banks were fairly effective in ending the situation, the credit card companies and especially the debt collection industry under pinning the credit card industry is particularly poor in stopping suspicious activity. That said, victim response strongly indicated, contrary to the general research, and a motivation of this research, that current red flag and breach notification laws did work, in several instances, and may be the only recourse at present to prevent every potential identity theft from turning into a completed crime.

Finally, it is clear that at present victims of identity theft respond to crime with shock and a sense of violation, and often bewilderment, indicating a fairly low level of consumer education. When, moreover, debt collection agencies become involved, and, worse, when the personal data is used to create official identity documents to then generate a false identity for a criminal who then commits another crime, the false data showing up on police criminal databases, the naïve response of police to apprehension of the person whose data has been stolen as if he or she was the criminal can only be said to amount to a revictimisation which makes the original crime much worse. As for victim response regarding law enforcement efforts at combating identity theft, their lack of confidence equals only offender dismissal in its impunity. Therefore, based on an analysis of their responses, it is determined that, in terms of the second factor of the situational equation according to routine activities theory, that the current target suitability for identity theft must also be deemed to be extremely high.

Finally, in terms of presence or absence of guardianship, this answer is divided between regulatory response and law enforcement response. Feeding in responses from offenders and victims, it was found that offenders dismiss as ineffective both regulatory and law enforcement efforts to stem the tide of identity theft, while it was found that victims felt that red flag and breach notification rules at least helped stop the crime from continuing, though they also found that law enforcement response was impotent and unhelpful. In terms of stakeholder responses, they generally continue to want to downplay identity theft and are content with current methods. Law enforcement at the precinct level, including the beat cop remains somewhat helpless in responding effectively to identity theft. The response given to one victim by an officer in a precinct was, because an identity theft had occurred in an international jurisdiction overseas, nothing could be done to assist the victim. This has become a common practice at the precinct level.

Moreover, the focus of the law enforcement paradigm on the small players, the small-scale identity thieves, usually individuals, has limited effectiveness. And of course it is true that even police lament the lack of serious punishment for this crime, and the fact that most sentences for even conviction are so short that they barely interrupt business as usual. At the same time, confidential discussion with personnel involved in special investigation units, both in the NYPD and Manhattan Attorney General's Office, as well as detectives working with the Secret Service and even Homeland Security, are acutely aware of the extent to which organised crime on a global level is involving more and more persons and increasing amounts of stolen goods and accounts, and that identity theft is becoming the crime of choice for organised criminals worldwide. As a result, details of a sample of a few investigations undertaken with these stakeholders working in cooperation with each other not only indicate surprise but shows a

determination in the discovery of every new twist or technique of identity theft devised by hackers overseas. There has been a greater number of apprehensions of small-time persons operating as recruits or mules in organisations known to be much more large scale and profitable to offenders. Once identity theft rises to the level of organised crime, other statutes can be included and will eventually become a more effective tool as an aid for prosecution. This will alter the global dimension and will ultimately include federal investigators in on cases, and then the crime is no longer viewed as minor, minimized or considered to be not a crime. At this level, it is also apparent that according to routine activities theory it is offender motivation and guardianship that need adjusting, reducing offender motivation, increasing guardianship, and punishment, as at this level it seems unlikely that there is anything a consumer, investor or wealthy individual can do, short of not banking money, to prevent this crime.

It is up to law enforcement to study the mechanisms of identity fraud and help banks devise more barriers and alerts in its system. Finally, it is important, that prison time for identity theft not be so minimal as to be dismissed, in terms of its deterrent effect, by identity fraudsters. By addressing these two pillars of routine activities theory, the escalating global crime of identity fraud can be combated more effectively by law enforcement. Organisationally, it is up to leadership in law enforcement to utilise new insight into the scope and seriousness of identity theft to realign all police departments as well as criminal justice policy and response to the cutting edge model currently being forged by the detective force specialising in identity theft.

It is important to note that there continues to be an identity crisis within law enforcement when it comes to combating identity theft. Every agency, local and national, wants to be considered “the best”. However, even the best of the best cannot stop identity theft until the crime is actually committed. I have only found one example of interdepartmental cooperation.

The NYPD and the Drug Enforcement Administration (DEA), a federal agency, has instituted a system known as SAFET Net, which helps investigators identify suspected individuals and locations that are under current investigative/observation. When either agency is conducting an investigation pursuant to an arrest, a check is done via the SAFET Net data base to ascertain if the cooperating agency has an ongoing investigation, in which a premature arrest might destroy months or even years of surveillance and/or case building by the other agency.

This creates a situation that may be labelled “lag time”. The crime gets reported to the victim, police or Private Corporation. In a significant way, the information conveyed to the police was not done efficiently. The victim experienced a time lapse which is put into the very system utilized by the agency due to the fact that most victims receive banking information on a monthly basis. The police then contact the private sector companies who do not cooperate. The employees claim it is confidential information, the civil liberty activists argue against police having “easy access” to people’s information, contending that it will lead to “Gestapo” tactics. This requires the police to go to the courts for a subpoena, which takes additional time to obtain the information from the credit card and/or internet provider. As time goes by the trail gets colder. The private sector companies apparently have a laissez-faire attitude because they are covered by insurance for their loss, and are concerned about bad publicity. This can frustrate the investigator, destroying morale, while the public also looses confidence in the criminal justice system. Hopefully, the use of the internet as a tool for the offender will become a tool to protect the victim.

Assuming that law enforcement has gathered the necessary information, problems arise concerning jurisdiction. Each agency, whether federal or local, wants to protect their domain. A lack of a central repository system, the desire and ability to share is the same problem that

plagues the investigation and control of identity theft. It also occurs in other criminal contexts but is more readily apparent in identity theft. A review of the policies and procedures within individual agencies in law enforcement uncover the egotistical and jealous safeguarding of their perceived images. Units and divisions stubbornly refuse to share information or share in the glory of (catching) apprehending identity thieves. For example, a highway patrol officer can stop an unknown or "wanted" identity thief (who is in possession with counterfeit identification documents) for speeding and have no idea of their true identity. The officer will run a check on the license plate and identification and if the results do not show the true identity of the individual being temporarily detained, that officer has no idea that he has encountered an identity thief. The Manhattan District Attorney's Office Detective Squad does not convey investigatory information to Precincts/Detectives or investigators from federal agencies. A precinct detective may have an individual being investigated for assault and that same individual may be under investigation as part of an international identity theft ring unbeknownst to the precinct detective.

Law enforcement has slowly and stubbornly began to admit that it takes team work to protect society. Some law enforcement agencies have begun to accept the role of academia. For example, during the early 1990's, a great reduction of crime was achieved in New York City when The Chief of the Transit Police Department, William Bratton consulted and collaborated with criminologist George Kelling, regarding Kelling's "broken windows theory of crime prevention." Drawing on this research, it can be argued that it is necessary to collaborate with academia in order to develop methods of combating and reducing identity theft.

A common argument within law enforcement is that identity theft is a typical, homogeneous crime. Ancillary crimes such as larcenies and those which fit into the white collar category tend to accompany identity theft. Law enforcement agencies do not possess the ability

to track identity theft crimes in a uniform way throughout government agencies. It is also well known within law enforcement agencies that there is neither centralized data nor comprehensive evidence which may be used as a law enforcement tool to rectify the identity theft problem. One theory as to the confusion of the identity theft problem is that the crime is not an individual one; it involves several financial and similar white-collar crimes (Hayward 2004). Copes et al. (2010) explained that various attempts using law enforcement records and victim surveys to measure identity theft have yielded inconsistent results. In spite of the on-going trend of identity theft, government agencies have not been able to use a much needed enforcement tool to combat the problem.

The continuous introduction of new media, technology applications and the use of the internet provides society with greater opportunities to communicate socially and to conduct business across the globe. However, these same technological benefits also present fraudsters with an ever-increasing array of opportunities to find unsecured loopholes through which to acquire personal information and to commit identity theft. Given a choice between committing an "unseen" crime such as identity theft or risk being 'seen" robbing a bank, it's easy to see why the former is preferred by fraudsters. In fact, it is not impossible for fraudsters, unscrupulous family members, acquaintances and employees to purloin one's identity. Identity theft is believed to be the white collar crime of choice in the United States during the past decade. The internet is not just the super highway for legitimate use; it is also a conduit for fraudsters to seek out victims just by the click of a mouse. It is a convenient way for criminals to prey on victims at limited costs.

Identity theft crimes can be difficult to investigate. Investigations can be cumbersome and time consuming. Some cases take years to conclude and in some instances, investigators are

aced with “ghost” cases that may never be solved. Most complex investigations are trans-national in scope reaching across multiple continents and jurisdictional boundaries. Investigators are often faced with scrambling to find language translators, uncooperative law enforcement governments which results in costly investigations because of the complexity of identity theft. Prosecutorial agencies, along with law enforcement are less likely to share responsibility for the enormous cost associated with investigating identity theft. Agency policies regarding reporting identity theft crimes to law enforcement and pressing for the prosecution of the offenders vary from inconsistent to prosecution. Additionally, investigators face rejection and un-cooperativeness from private companies whose employees are reluctant to report a crime or co-operate in criminal investigations. Quite often victims can be uncooperative during an investigation. This is a result of a lack of knowledge and available resources that victims are entitled to.

Some individuals who were interviewed within and outside of law enforcement revealed that companies fear of law suits charging false arrest, libel, malicious prosecution are greatly exaggerated and blown way out of proportion to the likelihood of their occurrence. This is particularly true when advance planning with legal counsel and/or security advisor covers procedures relating to investigating identity theft, interrogating suspects, gathering evidence, and determining its sufficiency. Obviously, avoidance of a no-prosecution policy does not necessarily imply that all offenses should be reported to law enforcement, because theirs is not a collection agency. The decision to press charges is often based on the intent of the fraudster and the amount of money that is involved. Neither justice nor the problems of an over-burdened criminal justice system are best served.

(i) Significance of Future Research

In order to implement an effective preventative program against identity theft**,** employees in the retail industry should be more alert in dealing with fraudsters in their daily duties. Some employees review store policy on rush orders and are constantly vigilant for suspect fraudsters. The law enforcement community is aware that the retail industry does not have effective provisions in place to stop losses on purchases made by card and identity theft fraudsters. Given the state of today's economy, customers are assigned credit limits. If an unusually large order from a customer exceeds their limit, a delay in shipment occurs until further information is obtained and the customer's identifying shopping history along with their address can be verified. Shipping department personnel can be instructed to report destinations that seem incompatible with the product being shipped. For example, a load of furniture destined for, or rerouted to, a machine shop should raise questions and draw attention within the store's security department.

Sales associates and other low level employees should not be too closely relied upon to produce sales in order to gain commissions. In doing so, those employees may be tempted to knowingly accept bad cards or bogus identification on orders, despite strong suspicions about the customer. There are some instances where associates were "assisting" the fraudsters by joining the criminal enterprises and accepting stolen identity data as verification for purchases in order to receive a benefit. The Federal government's response to the identity theft problem was a creation of a task force to locate the needle in the haystack. The investigations are labour-intensive and generally require a staff of detectives, agents and analysts with multiple skill sets. When a theft involves a large number of potential victims, investigative agencies often need additional personnel to handle victim-witness coordination. Local law enforcement officers, regardless of where they work, express the challenges of multi jurisdictional investigation and prosecution of

identity thieves. My source at American Express feels that investigating identity theft is laborious and time consuming, with “not enough time in a day” for investigators to conduct their investigations because there is an abundance of paper that must be evaluated.

As today’s organizations continue to utilize all of their resources in order to minimize the occurrence and impact of identity theft and some have asked for support of a risk-based, national data security and breach notification requirement program. An approach that encompasses effective prevention, public awareness and education, victim assistance, and law enforcement measure, and fully engaged federal, state, and local authorities will be successful in protecting citizens and private entities for the crime. A more effective law enforcement tool against identity theft is training. Unless law enforcement is trained and frequent the subculture they will be forever lagging behind this fast paced crime.

Many victims who were contacted would rather not follow through in assisting the police or prosecutors to bring an accusatory instrument against identity thieves. They feel that once the crime is committed and they are not physically hurt, their daily way of life can be resumed. In New York City, the majority of cases are plea-bargained because of the backlog of cases in the Court system. Neither the police nor the prosecutor has the time to spend on cases that are adjourned once per month for approximately one year. They themselves would rather seek a resolution on cases as quickly as possible in order to move victims and defendants along and most importantly, it becomes a cost cutting measure given the anaemic state of the economy.

As identity theft continue to evolve, qualitative and quantitative studies of the offenders and victims characteristics, methods, as well as what measures, if any, the criminal justice system have taken to alleviate the identity theft. This researcher will continue to analyse data from this

thesis in order to further delineate why and how the broken criminal justice system is unable to cope with the methods use by the offenders to commit this crime against their victims.

A combination of the factors discussed in the previous paragraphs show the environment in which offenders continue to operate. The convergence of these factors has been discussed. If the aforementioned issues are not acted upon, all factors when combined suggest that identity theft will continue to evolve.

APPENDIX 1

LISTING OF TABLES

APPENDIX 2

Victim's Questionnaire

The below listed questions were proposed to twenty-five victims who participated in this study. All answers can be found in table 2 of the thesis.

During the past two years have you or anyone you know have discovered that someone:

1. Used or attempted to use credit cards or information without permission?
2. Used or attempted to use any other existing account(s) such as bank accounts or debit cards, or checks without your or the account holder's permission?
3. Attempted to use information to obtain new loans, incur debts, open other accounts, or to commit other crimes?
4. Did these actions occur separately or simultaneously?
5. Which incident of identity theft was quickly discovered?
6. How did you become aware of the theft?
7. What was the total dollar amount of the theft?
8. Have the misuse of the various account(s), forced you, a family member, or a friend to close any accounts?
9. How much time did you spend cleaning up your record?
10. Have you or anyone you know had utilities cut off, been a subject in a criminal investigation, gotten hurt, or forced to close accounts because of misuse?

APPENDIX 3

Offender's Questionnaire

The following is a sample of questions prepared for interviews with offenders/Respondents:

1. How did you rationalise what you were doing?
2. Why did you choose to offend as an identity thief?
3. Why did you choose to steal identities at that time?
4. How did you get the idea of stealing identities?
5. When did you get into stealing identities?
6. Why doesn't everyone steal identities?
7. What have you learned?
8. If you knew other offenders would you have been able to do things differently?
9. Did you think you would be caught?
10. Did you do anything stupid and was caught?
11. What made it possible for you to for you to do the crime on the street or on line?
12. Did you have a prior relationship with your victim (s)?
13. Were you aware of your victim (s) identity prior to carrying out the theft?
14. Did you calculate the risks involved with fooling around with other people identities?
15. Do you fear serving time in prison?
16. So, why did you choose ID theft?
17. Why did you choose those methods?
18. weren't you afraid of being caught?
19. on the victims?
20. Such as?
21. What makes you tick? Tell me about yourself.
22. Why are you facing deportation?
23. What do you know about Id's and the way people go about stealing them?
24. Why are you locked up?
25. Does anyone object to doing a group interview?
26. If you didn't know the recruiters would you have done things differently?
27. You are young… how did you get involve in ID theft?
28. What was probation like?
29. Why take the risk of going to prison?
30. Why did you choose to do this at your tender age?
31. What have you learned from your experience?
32. Why did you get involved in this theft ring?
33. Didn't it occur to you that what they were doing was against the law?
34. Tell me about your group?
35. The threat of being arrested didn't mean much to you?
36. Are you concerned about re-offending?

37. I learned that you were involved with an ID theft group?
38. Weren't you afraid that your victim's life would be ruined because of this?
39. How would you feel if the shoe was on the other foot?
40. What exactly did you do with the other shoppers?
41. Did it occur to you that someday this would unravel?
42. But why take the risks of impersonating someone else
43. So you have an ID theft issue?
44. What have you learned if anything from this crime?
45. I understand that you were a shopper for an organized group?
46. Why didn't you stop and notify the authorities?
47. I see you are no stranger to the court system. Why can't you stop re-offending?
48. You are telling me that ID theft is not as bad as a robbery or murder?
49. What happened at Chase Bank?
50. Were the employees aware that their actions were illegal?
51. Why would those employees take such risks?
52. What extent are you aware of the amount of identity theft in society and on the internet?

APPENDIX 4

Law Enforcement Questionnaire

All questions in appendix 3 were asked of Law Enforcement Personnel and Private Industry Professionals

How often does identity theft occur in your precinct?

1. How seriously is identity theft addressed in the precinct?
2. How many persons were involved in the identity theft crime?
3. To what extent did the crime extend beyond jurisdiction to the global dimension?
4. What dollar amounts were involved in the crime?
5. What techniques were involved in the crime?
6. How many persons total were arrested as a result of the detection of the crime?
7. What have you done to prevent identity theft on line?
8. Have the police adjusted to the focus of the problem?
9. Are the thieves becoming more sophisticated in accessing personal data?
10. Is the government obligated to protect its citizenry against identity theft??
11. Do you have the tools to combat the identity theft problem?
12. How you can be more effective in preventing, arresting and prosecuting identity thieves?
13. Do you think that current laws are adequate?
15. You cannot act until a complaint is made. What level of cooperation do you need to be effective at this stage?
16. Do you perceived identity theft to be different from other crimes?
17. Should current laws be modified or proposed?
18. Are current lawmakers on the state and federal level proposing effective legislation?
19. Is there duplicate reporting of identity theft crimes?
20. Are identity theft crimes being under reported?
21. What is the working relationship between agencies?
22. Are there dedicated identity theft units within your agency?
23. Do you have substantial knowledge of how the identity thieves operate?

APPENDIX 5

Additional Interviews with Offenders/Respondents

During the course of this research interviews were conducted with 25 offenders/ respondents. The official names were obliterated to secure the anonymity of all respondents. Therefore, it was more practical to refer to all respondents by a letter from the alphabet, A through Y. Additionally, all questions asked by this researcher are reflected in italics. Some respondents, such as, A and B were interviewed twice after a break in the conversations.

(A)

Joe: "I started working for one of the families (the syndicate) ... went to jail a couple of times for not doing my thing with common sense. It was in jail that I changed my life around for the good of my wife and kids. I met somebody in the can who introduced me to stealing identities ... decided to get involved in stealing identities after I realized that I could make money using people's information such as name, address, Social Security number, driver's license number, mother's maiden name, and date of birth. JN: *Did you calculate the risks involved with fooling around with other people's identities?* Yes. But at the time I also learned that a mother's maiden name was the best piece of information you could get to apply for a birth certificate because you could do a lot of things like ... apply for any help to get welfare and food stamps ... make up IDs to trade or sell or use it for yourself so that when the DTs (Detectives) catch you... they think you're clean."

After taking a quiet moment, Joe further spoke about the documents that he acquired from stealing people's information.

Joe: "I and my friend surfed the Internet for websites, which buy personal information. I scanned all the information with the Social Security numbers, dates of births, driver's license numbers and whatever I could find. I sent about 10 to 12 sheets of information to the Internet (website) addresses twice per week and they sent me $600 per batch of stolen stuff through Western Union. From the very beginning, I learned that the risk of getting caught and doing time is very low, but the profit is good. Me and my boys know that most of the times the cops take a long time to catch up to us and it is even longer when people live far away from each other so they don't want to be bothered travelling to testify against you. This is just easy to do with lots of opportunities to make good money. Most of the times the Judge will give you probation or community service, even if the DA ask for jail time for you. *Do you fear serving time in prison?* Not really...if me and my boys have to go to Rikers (jail) for a little while ... we can get good practice when we are in cause ... there is a market for everything you trade in the can."

(B)

JN: *So, why did you choose ID theft?* Bobby: I am not a real ID thief. I only got into this because it was part of the ceremony for my gang initiation. We had to prove that we could steal IDs from people. If you were good at it, they would initiate you pronto and

it became your speciality as part of your job. We broke into apartments, houses and cars so that we could take whatever information about a person we could find. *Why did you choose those methods?* Cause they were all easy to do. We worked four at a time and had to have a girl with us... they distract other people and can pretend that they always need help with anything... they don't get too nervous and they keep their voices the same tone. We hit (burglarized) houses late in the morning hours after rush hour because most people go to work and kids go to school. *Weren't you afraid of being caught?* No. Cause we pretended to be landscapers or delivery people. We drove around the neighbourhood and watched for people to leave their houses... then we went in through a back window or door and then we would let everybody in. We took information on credit cards, safes, family photos, mobile phones, birth certificates and utility bills ... sometimes; we would even take whole drawers of paperwork. After we brought back the looted information to the person who was responsible for processing out what was needed to start making IDs, then other people hacked into websites on the net to get credit bureau reports. *On the victims?* Uh huh.... once we got that information, other kinds of bogus Id's were made up. *Such as?* Credit cards, car loans and then we applied for duplicate Social Security Numbers. Some gang members were trained to be shoppers. There were the ones who bust out the credit cards at big stores like Bloomingdales, Macy's, Saks Fifth Avenue and Apple. They bought all kinds designer merchandise like, Lalique´ perfume, Louis Vuitton bags, belts, shoes, watches and jewellery. They shopped for cars that were immediately shipped to countries in Eastern Europe, parts of the Caribbean and Central and Latin America.

(C)

JN: *What makes you tick? Tell me about yourself.* Michael: When I was 17, I started out as a lush worker and rode the subways in New York from the beginning of the line to the end searching for people who were drunk. I always had a razor for protection ... so I cut their pockets ... some ... I just turned their pockets inside and out, took their wallets or pocketbooks, emptied everything inside my knap-sack and split. Sometimes I would go down to the Union Square Station at rush hour ... and learn to pick the passengers pockets ... Cos the train used to be packed ... business was good for me. Sometimes, if I got caught, I pretended that I couldn't speak and they (the police) would let me go. One day I rode the trains all night and couldn't make any money because the new class of rookie cops was riding the trains. They cramped my style. I needed money and so the following day, I sold as much information as I could to another thief who took me to an address in located in a basement, the Bronx and they made a driver's license and two credit cards for me ... They hit me up for $25 for the IDs. I used one of the credit cards to rent a room in a single room occupancy hotel for me and my girlfriend for about two weeks before we moved on to another hotel. About eighteen months later, my luck ran out on me ... a group of decoy cops who were doing a sting operation against lush workers finally caught up to me... I was locked up and the Judge sentenced me to one and a half to three years ... No I am facing deportation back to Jamaica. *Why are you facing deportation?* Cos ... Me nah citizen ... Me from Jamaica man.

My informant, Charlie Hustle, introduced me to five of his old friends, who are also ex-

(D)

JN: *Now... let's talk Harold... what do you know about Id's and the way people go about stealing them?* "I and my friends go through dumpsters outside of hotels to collect cans so that we can take them in for money. One day I found a letter with a credit card in the dumpster. I didn't know what to do. I looked for my friend and showed him the letter and the card. He was undecided about what action he should've taken with the information that he held. We went to a store on the west side of 42nd Street ... gave the credit card and the letter to the guy behind the glass partition ... paid $55 and walked out with a another credit card in my pocket." (Harold)

Even though Harold swore that he did not intend to go into the identity theft business, his journey continued. He further explained,

"I started stealing cell phone bills from unlocked mail boxes. Then I would reroute mail to my friend's addresses by filling a change of address card at the post office... then I made a lot more new identities. We sold the IDs to illegal aliens and to people who like to shop. The shoppers sold their things to bodega owners in Washington Heights, Manhattan." (Harold)

(E)

What I needed were at least two people to help me make money. I chose a "working" couple whom I knew from back in the day when we did robberies together. I knew the woman was good at busting out credit cards. The couple had recently received an eviction notice so they could use the cash. The cards came from a "mill" on the upper west side of Manhattan. The price of cards varied from $500 to $700 each with a limit of $10.000- $15.000. We specialized in buying electronics for resale to smaller electronic stores in Washington heights and the Lower East side of Manhattan. Resale prices were agreed upon prior to picking up the merchandise. It was the safest way to fly under the radar and collect cash. I had arranged for my girl to get a job as an accounts receivable worker at a large electronics store that carried the inventory that I needed for resale. Each day my girl kept me abreast of the hottest ticket items that were scheduled for store delivery. Twice per week for six months, the couple went to the store, bought the selected merchandise with a different credit card and walked out. I waited outside of the store with a truck. When the transaction was completed, I received a phone call instructing me to pull my truck in front of the store. The merchandise was loaded into the truck and taken to the smaller stores for resale. The couple received 20% of the resale value of each electronic piece. The most requested items were cameras, cell phones, computers, fax machines, high-end speakers and head sets. For me, this was a better way to earn a living. It was easier, cleaner and when the job was done no one got hurt and we never had to worry about the police.

(F)

JN: So you came from the City of Angels? (Pueblo?) Yes. I paid someone to take me across the border to America. *Why are you locked up?* I came here looking for work, could not find work. I needed lots of money because I have a wife and two children back in Pueblo. I must also pay off the money I still owe for the transport across the border. My cousin told me about an easy way to make money and I joined with him to make ID cards. I like it because it was easy money. I paid the rent and sent money back home every week. It was 13 other people

doing it. The boss brought the plastic and his friend gave us the names and numbers every morning. We worked for about 6 hours every day in a basement in Queens. I made lots of cards about 70 everyday. I sometimes we used old cards when the numbers were still good. We just changed the names and polish the card so that they would look clean. Sometimes I took orders for cards over the phone or the internet. People paid different prices for cards. It depends on if the boss is in a good mood that day. Most days they sold them for $400.00 each. The value was like $5.000. Sometimes I had to take boxes of cards to the Port down by the dock. I gave them to Joe and he sends them overseas. *Were you afraid of being caught?* The boss said not to worry about anything because his brother works for the NYPD and if we get caught we wouldn't have to worry. That is not true.

(G-L)

JN: Does anyone object to doing a group interview? NO. The main spokes person for the group explained. We were all part of a cyber crime ring that originated in Eastern Europe. Some of us came to the US pretending to be students, Au Pairs and other workers. The recruiter lives in Russia. We were all recruited from the Internet with a promise of making a lot of money. Everyone was given ID cards, driver's licenses, a credit card and passports, a plane ticket and instructions to meet our leader here in the US. Everyone received new passports and was instructed to open bank accounts. Innocent people's and businesses accounts were hacked, passwords to banking information were used to transfer money into the new accounts and then we were told to withdraw the monies from the accounts. After we took the money from the bank, we travelled to Russia with the cash, gave it to the big man and were paid sometimes very little for taking the risk of getting arrested like we are now. The federal agents said that if we cooperate with them, we would do much better. But no one is going to say anything because we have families back in our countries and everyone knows that the Russian mob is running this business. It is a real business because this is what they do all of the time. We felt that this was a good thing to do because there was no work for us to do back in our countries and it sounded very good to us. We knew that eventually we would get caught but we thought that if we told the authorities that we did not speak English they would send us home on a plane so that we would not spend time in a US jail. *If you didn't know the recruiters would you have done things differently?* Not really, because everyone that we know is trying their hands at this. It is another way to make money.

(M)

JN: You are young… how did you get involve in ID theft? I was always in the system. My parents died when I was 2 and I lived in foster homes. When I was 16 I ran away and lived on the streets. My pimp kept beating me up and taking my money and at age 18, I stabbed him. I was arrested and served time on probation. *What was probation like?* They did not help. It was nothing positive for me. When I was arrested I met someone in jail who introduced me to her organization. They were protected by a known street gang. I felt that I needed that kind of protection also and so, I went to work for them. *Why take the risk of going to prison?* It worked for me. I travelled throughout the country as a shopper with different groups. It was fun living on the edge and not getting caught and at times almost getting arrested. I like to work in Ohio and California because when we went into the expensive stores they hardly checked Id's. I worked in a team. We were given credit cards and Id's with our pictures on them. The leader in the team took orders for specific merchandise over her cell phone. We would then choose which items we wanted to buy. There was always a transport van to drop us off at the stores. The pick-

up areas was always different from the drop off site. We kept in contact with throw away phones. I liked to buy Hermes handbags. That was my speciality. It reminded me of the things I did not have growing up. I shopped in every major city in Ohio and California. I was given nice clothes to wear and was told how to speak and act when I went into the stores. At the end of the day the group leader took the merchandise from me and left in another van that was packed with items. I was taken back to a hotel to rest up for the following day. Every day I received a different credit card with ID. One day, I came back to New York, went to Sachs Fifth Ave, was attempting to buy a Louis Vuitton handbag, the clerk got suspicious, called for security and they arrested me. When I went before the Judge, I thought he was going to give me a lot of jail time but he acted like he didn't care what I did, how I did it or anything. I know that they don't think this is a serious crime and I will be out of here soon.

(N)

JN: Why did you choose this crime? I needed money, it's easy to do, I will hardly jail time and it helps with the rent. *How did you choose your victims?* My girlfriend works in a pharmacy so she can put her hands on everybody's information. All she has to do is bring it up in the computer. She gives me the client's information and I sell that information to an acquaintance for $1000.00 per batch of names and information. We have a child to take care of and things are bad out there. *Why doesn't everyone do id theft?* Some people are afraid and they don't want to risk getting caught and going to jail. I am not afraid it is not as risky as you think it is. You could go on the net and do this and get away with it. If you get caught you will probably get probation. Nothing happedto me. I got a conditional discharge.

(O)

JN: Why did you choose to do this at your tender age? In the beginning, I was scared but I got pregnant, could not even let my parents know that I was pregnant. I needed money for an abortion. My boyfriend at the time said it was safe because nothing was going to happen to me. I had to go around shopping in big department stores with the Id's and credit cards that he gave me until I got caught up in a ring that went from New York to California. Even though I was pregnant he made me shop for hours until I could not shop any more. I ended up having my baby in here (jail). I did not make out as good as he did. *What have you learn from your experience?* I learn that if you want to commit a crime you should do it yourself and don't follow others.

(P)

JN: Why did you get involved in this theft ring? The risks are low and the rewards are high. I am better off doing ID theft than a stick up job. I see what my friends have. They always have money, wearing nice clothes and I have no job so I wanted to get a piece of the action. *Didn't it occur to you that what they were doing was against the law?* I didn't look at it this way. It just seemed like a way to make easy money. No one was getting hurt. It's not like they are using guns, knives or anything. Before I was arrested I worked as a look-out for people who travelled up and down the East coast busting out credit cards and passing checks. ID theft is a good way to hide from the police. Everyone in the ring that I ran with have a record so the only way that we can fly under the radar is to get new Id's. It's all good because all of the money is covered by insurance. The group that they put me to work with does not stay in one place too long they keep moving us so that the people in the stores won't get to know us. There are generally 6 to 8 people per group. The women mostly do the shopping for high end merchandise

like perfume and designer items. We guys have to make sure that they are safe and everything. Somebody is always sitting in the van so that they can store all of the things in there. Then later on the group leader will switch vans and take away the things that they buy that day.

(Q)

Offender Q is a police informant who is currently serving a 5year probation term for identity theft. Initially, Offender Q agreed to talk to me and later changed her mind. I advised her that if she decide to move forward with the interview in the future I can be contacted via my telephone number.

(R)

Tell me about your group? My boyfriend was the leader of a criminal group that focused on buying genuine Apple products for resale. I was in charge of all of the shoppers who bought the products. I searched web-based portals and bought names, credit card accounts numbers of ID theft victims. That information was then used to produce counterfeit credit cards. Shoppers were then recruited and given credit cards with their real names and the stolen numbers. I then gave the shoppers a list of Apple products to buy. They were all electronic products. *Were you afraid of getting caught and going to jail?* No because we had a secured system. *How did you feel about Apple losing money to your shoppers?* It was no big deal. Apple has insurance to cover their missing merchandise. They really don't care about that. *What items were purchased?* iPods, iPads, gift cards and MacBooks. *What locations did the shoppers hit?* They shopped at stores in the Midwest and along the east coast. *Now that you have been arrested, what have you learned from this experience?* I will get very little jail time for getting involved. The credit card companies will cover everything it's not like one person is paying for it. The most time I may get is about 4 years even though we made millions of dollars off Apple.

(S)

JN: The threat of being arrested didn't mean much to you? From a teenager, I was very good at surfing the net and findings anything that I wanted. My uncle was in the computer business and he taught me a lot about them. I did not like to work but I needed money, fast cars and girlfriends. The best ways to do all of those things was to look where I could find the income to do whatever I wanted. I went to a school in my village and learned how to crack computer codes and fish for financial information. In the beginning, I was no good. It was frustrating but I kept practising for long hours every day until I got better at it. My best method was to study the Forbes 400 list for people with expensive accounts and property information that was available on the net. I looked for the amount of their lines of credit and the amount of mortgages they owed. At that time, the best people to go after was the ones who had ties to Silicon Valley because of their net worth. I created about a dozen cyber identities. My most successful ones were "Topfinancegroup", "stayintheshadows" and "universalescrow". As a Russian citizen living in Russia, I felt that I would never be caught and I would continue to make money, live like the rich guys in Silicon Valley and retire at age 50. My best means of communicating was by e-mail and instant messaging. It was not difficult to advertise via the net for partners in the United States to work with me. Career Builder.com was my most successful cite to advertise for working partners. Within a four year period, I joined in partnership with a dozen individuals in the US. They were all willing to make money via the net. We agreed to split the profits when each job was done. I kept folders with personal information on the people that I targeted and hired private investigators when I needed additional information to complete

my folders. Once that was done, my recruits travelled throughout the US to financial institutions with the necessary copies of fake transfer request forms, power of attorney paperwork and whatever was needed to complete a transaction for me. Fake or stolen credit cards were used to pay for travel expenses. The transfer request forms were used to transfer money to accounts bearing the "workers" names and then transferred to accounts bearing my name. Several million dollars was sent to my Russian accounts. I was eventually tricked into coming to the US to do a large transaction and was arrested in New York. I am not concerned about doing the time. It is comfortable in the New York jail. The meals are ok. The recreation areas are decent areas to work out in and nobody bothers me. Besides, they feel that I am a Russian spy. The Judge gave me three to ten years in prison. I will complete that and go home. I will still have a comfortable life there. *JN: are you concerned about re-offending?* I am not. Life is good. I am not hurting anyone. Life could've been worse.

(T)

I learned that you were involved with an ID theft group? I was. It was a quick way to make a few extra dollars to help pay the rent but I see it didn't work out because now I am in here. *Weren't you afraid that your victim's life would be ruined because of this? No*. Never gave it one thought. The people in the ring said that no one will be harmed by this. *How would you feel if the shoe was on the other foot?* ….I really doesn't know. I guess I would be pissed off and I would want to go find the person who did this to me. I am now facing 1 year for something that wasn't worth it. I am ruining my life because of a stupid thing. I need to think. They recruited me to help them shop and it didn't even pay as much as it should. *What exactly did you do with the other shoppers?* I went along with them to some very nice stores. One in particular called Apple was different. Other girls did the buying and I help carry the bags back to the van. I was only working with them for about three months. It's not like I made a big profit or anything. My salary was $250.00 per week part time.

(U)

Let's talk…. I came into the US as an illegal immigrant from Haiti and I needed working papers in order to start driving at a limo company. *Did it occur to you that someday this would unravel?* Not really because I know other people who have been using stolen and bought Id's for years now and nothing happened to them. 7 years ago I bought a dead person's ID for $2500.00. They say it was solid and good. I needed to find a job that pays good money because I have two families back in Haiti to take care of. *But why take the risks of impersonating someone else?* I am doing it for good reasons. I pray every day that everything would be ok. Every day I go to work, I am very careful not to do anything to anybody. I obey all the rules until I had an accident. When the police came they asked me if I was a citizen and I told them I was a resident. They got suspicious and ran this name in the computer car. After a while, they came and said that there was an alarm out for this dead man's identification. I was arrested and received 6 months in jail and is now facing deportation. I am an innocent man. I did not hurt anybody. The man is already dead and they want to send me back to Haiti. What am I going to do there?

(V)

So you have an ID theft issue? Yeah…. When I was a teenager my parents sent me to live in a foster home. When I was there, I always got into trouble in the local town. One night when my room mate was in the shower I looked into his wallet and took his ID. The next morning I

found a place that made Id's so I got them to put his information with my photo and ever since then I always use the new name for ID. I applied for government benefits under the bogus ID without a problem because my ex room mate was in jail for a long time. One day the police picked me up for identity theft. My ex room mate got out of jail and also applied for assistance when they told him that he could not get it because someone else was already getting assistance under his name. *What have you learned if anything from this crime?* You can run but you can't hide. Even though I wasn't hurting anybody they still got me.

(W)

I understand that you were a shopper for an organized group? I was a shopper but I thought it was no big deal. They asked me if I wanted to make some fast money and that it was safe. I knew the summer was coming soon so I wanted to buy some new things so that I and my friends could roll with. That's why I was recruited as a shopper. I did a little bit of travelling to state like Florida and Ohio. At first it was fun but then it started to play out because I knew that I could not go on like this. They made me feel uncomfortable. I was worried that one day someone would see me and call the police. I had never been locked up before. My boyfriend went to jail for stealing someone's identity so I had no intention of doing the same thing. I was beginning to think that it was too risky and it was not worth it to getting caught. My parents would disown me end everything. *Why didn't you stop and notify the authorities?* I did not want to be a snitch because snitches get ditches and I was making decent money every week. My pay for five days was $800.00 and sometimes if you see something that you like they would get it for you and charge you a discount for it. My role was to buy Lalique perfume. I was trained to bust out every credit card that I held in my hand. If I went to a perfume counter to buy such an expensive perfume and the attendant became suspicious I would try to sweet talk her until she calm herself down and then pull out the card for the purchase and verification of my ID. I was always jittery when they checked my ID and would scope out my escape route when I enter every store. This lasted for about 13 months before I got busted. I am going to jail for 6 months with 5 years probation.

(X)

I see you are no stranger to the court system. Why can't you stop re-offending? You are talking about the old days when I was crazy and did bad things to people. I don't do those things any more. *You are telling me that ID theft is not as bad as a robbery or murder?* It really is not. Nobody gets hurt in this thing. Nobody have to go into their pockets like the way it used to. This is a victimless crime and that is why I tried my hand in it for a little bit. I was one of the recruiters for the group. They asked me to give them a hand because I have been around a long time and they know that I can take care of myself while looking out for them. I watch all these kids grow up so I know who to trust from whom not to turn my back on. Before I work on the new people I am very good to them. I offer to buy them whatever they need and everything. The thing is to let them get close to you. They have to gain your confidence if not; they will disappear and run their mouth about the business. For the young recruits, it is an exciting time in their lives because they are now being exposed beyond their universe. Being involved in the ring is not all that bad because you have protection while collecting a salary. It's hard to stay away from this kind of life. It's all I know about. This is definitely not robbing anyone. I train the new recruits how to be business savvy yet forceful. They need to know how to be alert at all times just in case the cops or security is looking at them. It is also very important for them to be

polite and friendly with every one they do business with because the closer they get to the people in charge the more trusted they become.

(Y)

What happened at Chase Bank? I was part of a group that took over $1 million dollars from Chase Bank. We were approached by pickpockets who offered personal information in exchange for money. The information was verified by two employees at the bank. *Were the employees aware that their actions were illegal?* Of Course, they were in on it? *Why would those employees take such risks?* When the money is good people will do anything. Anyhow, fraudulent transactions were taking place at the bank with the victim's personal information. Credit cards were manufactured in the victims' names along with driver's licenses. What role did you play within the group? I passed along the stolen information to get new credit from the credit agencies. I am not too worried if I spend a little bit of time in jail, I'll be home by Christmas.

APPENDIX 6

Glossary of Legal Terms as Applicable to an Offender in the Court System

ACQUITTAL: A disposition of a case in which the defendant is found not guilty.

ADA: Abbreviation for Assistant District Attorney. See also Assistant District Attorney.

ADJOURN: To suspend a proceeding to a later time and perhaps different place.

ADJOURNMENT IN CONTEMPLATION OF DISMISSAL (ACD): A conditional dismissal of a case pending law-abiding behavior of the defendant. An ACD case may be restored to the court's calendar if the defendant commits any new crimes. A defendant is not required to enter a plea of innocence or guilt. The case is adjourned for six months, or 1 year for family offenses or marijuana cases.

AFFIDAVIT: A written statement of facts submitted in the course of a legal proceeding. See also corroborating affidavit.

AFFIANT: One who makes an affidavit.

ARRAIGNMENT: An early stage in the criminal justice process, occurring after an arrest. The defendant is brought before a judge and informed of the charges pending against him or her. If applicable, bail is set.

ARRAIGNMENT COURT PART: The location in which defendants are arraigned. In Manhattan, the majority of defendants are arraigned within 24 hours of their arrest. Defendants are initially arraigned in Criminal Court on the felony or misdemeanour’s complaint. Defendants who are later indicted by a Grand Jury will be arraigned again in Supreme Court.

ARREST: In the majority of cases, an arrest is the first stage in the criminal justice process. In some cases, an investigation precedes the arrest. In a typical arrest, a defendant is charged by the police and taken into custody.

ASSISTANT DISTRICT ATTORNEY (ADA): Assistant District Attorneys are lawyers hired by the District Attorney to prosecute cases as representatives of the People of the State of New York.

BAIL: Cash or bond posted by a defendant as collateral to ensure that he or she returns to court on a future date.

BENCH WARRANT: A warrant issued by a judge when an individual fails to appear in court at a specified date and time.

CALENDAR PART: Court Part to which a case is sent after arraignment, but before trial. Motions and pleas are heard in this Part.

COMPLAINT: The legal instrument filed by the State which initiates a criminal action. The complaint states the alleged crime of the defendant in legal language. In Criminal Court (misdemeanour's cases), the complaint serves as the formal accusatory instrument. In Supreme Court (felony cases), the complaint serves as a preliminary accusatory instrument until a Grand Jury indictment is obtained.

COMPLAINANT: A person who makes a complaint or files a formal charge in a court of law.

COMPLAINT ROOM: See ECAB

CONDITIONAL DISCHARGE: A sentence imposed by a judge when a court believes that neither jail nor probation is appropriate for the defendant. The court can require the defendant to lead a law-abiding life, to participate in a specific program, make restitution, perform community service, or to avoid contact with certain persons. If the defendant does not complete the condition, then the court can revoke the sentence and re sentence the defendant.

CONTRABAND: Goods barred by law. Contraband generally includes specific weapons or drugs prohibited by law.

CONVICTION: A disposition of a case in which the defendant is found guilty by trial or plea.

CORROBORATING AFFIDAVIT: An affidavit provided by a witness that confirms the witness' assertions as stated in the criminal complaint (the legal instrument which initiates a criminal action). A corroborating affidavit converts a complaint into an information, which is then ready to proceed through the criminal justice process. It must be subscribed and verified.

COURT CLERK: The Court Clerk assists the judge in record-keeping and other clerical duties; generally in charge of the personnel assigned to the courtroom.

COURT OFFICERS: Court officers are distinguished by their uniforms, badges, and shoulder patches and they are responsible for security in the court room. They are usually armed. They often assist the clerk of the court with clerical duties.

COURT PART: The physical location, a court room, in which court proceedings occur. See also Arraignment Part, Jury Part, and All Purpose Part.

CRIMINAL COURT: In New York City, the court in which misdemeanour's and violation cases are handled.

CRIMINAL COURT ALL PURPOSE PART (AP PART): The Criminal Court part in which various proceedings occur between arraignment and trial. Motions and pleas are handled in the part.

CROSS-EXAMINATION: The questioning of a witness presented by the opposing party at trial.

DECLINE TO PROSECUTE (DP): In some cases, the prosecutor may decide not to proceed against a defendant, in which case the prosecutor declines to prosecute the case. A prosecutor may decline to prosecute for a number of reasons, for example, if there is insufficient evidence or if further investigation is needed.

DEFENDANT: The person alleged to have committed the crime.

DEFENSE LAWYER: The lawyer who represents the defendant in a criminal case. The defence of those who cannot afford to pay for a lawyer is provided by organizations such as the Legal Aid Society in New York City and a few other counties, or the Public Defender's Office in some upstate counties, or by private attorneys assigned by the court.

18(b) LAWYER: A private lawyer who is appointed to represent an indigent defendant where there is no Legal Aid Society or Public Defender's office, or where these agencies are unable to provide representation because of a conflict of interest or other policy decisions. 18(b) refers to Article 18(b) of the County Law, which authorizes the appointment and payment of private attorneys with county monies in criminal cases.

DEPARTMENT OF CORRECTION: The New York City agency in charge of all persons in detention. Department personnel can be identified by the badge that says "Dept of Correction" and a pin in their collar saying "DC." This department also transports prisoners to and from court.

DEPONENT: A person who testifies under oath, usually in writing.

DESK APPEARANCE TICKET (DAT): A DAT is issued for less serious crimes. It releases a defendant from custody before arraignment and requires the defendant to appear in Criminal Court on a specified day for arraignment. If a defendant fails to appear on a DAT, a bench warrant may be issued. The warrant authorizes the arrest of the defendant and the arresting officer is directed to bring the defendant before the court.

DISMISSAL: The disposition of a case in which the charges against a defendant are removed. Only a judge can dismiss a case.

DISPOSITION: Once a case has concluded, it is said to be disposed. Possible dispositions include: conviction by trial or plea, dismissal, and acquittal.

DISTRICT ATTORNEY: The District Attorney is a lawyer, elected by the residents of his jurisdiction, to represent the State in criminal proceedings against those accused of crimes.

DOCKET NUMBER: Cases are numbered, and tracked by the Court with a docket number.

ECAB: The District Attorney's complaint room, also known as ECAB (Early Case Assessment Bureau), is where felony and misdemeanour's cases are evaluated and complaints are drafted by ADAs. ADAs staff ECAB seven days a week.

FELONY: An offence which is the most serious crime category. Felonies are divided into five classes: "A", "B", "C", "D", and "E" An "A" felony is the most serious, and an "E" felony is the least serious. The class determines the permissible sentence and prison terms in excess of one year that may, and sometimes must, be imposed. Examples of felonies are robbery, burglary, grand larceny, sale of narcotics, and murder.

GRAND JURY: Under New York State law, Grand Juries are empowered to hear evidence presented by prosecutors and to file charges, known as indictments, in felony cases. The Grand Jury can also conduct independent investigations. Each Grand Jury is comprised of 23 people.

HEARSAY: Evidence based upon the reports of others, rather than on the first-hand experience of a witness.

HUNG JURY: A jury that cannot reach a unanimous verdict is called a hung jury. When there is a hung jury, the case may be retried.

INDICTMENT: A written statement charging a party with the commission of a crime or other offence, drawn up by a prosecuting attorney, and voted and filed by a Grand Jury.

INFORMATION: A complaint which has the necessary corroborating affidavit.

INTERPRETER: Provides translation for non-English speaking witnesses and defendants.

JUDGE: Presides over trials and hearings, decides motions, and conducts arraignments.

JURISDICTION: The territorial range over which the authority to interpret and apply the law extends. Each of the 62 counties in New York State has a District Attorney who is an elected official. Each DA has jurisdiction to prosecute crimes and offenses that are committed in the county of election only. The City of New York contains five counties and has five District Attorney's Offices: New York County (Manhattan), Kings County (Brooklyn), Queens County (Queens), Bronx County (the Bronx), and Richmond County (Staten Island).

JURY PART: Court Part in which trials occur.

MISDEMEANOR: Misdemeanour's are offenses for which a term of up to one year may be imposed. Misdemeanour's are divided into two classes: "A" and "B." The maximum term of

imprisonment for an "A" misdemeanour's is one year and the maximum term for a "B" misdemeanour's is three months. Examples of misdemeanour's are shoplifting, trespassing in a building, and jumping a turnstile.

OFFENSE: In New York there are three major classes of offenses for which a person may be prosecuted: violations, misdemeanour's, and felonies. Violations are the least serious offenses. Some are defined in the Penal Law of New York State and others can be found in statutes such as the Vehicle and Traffic Law or in local ordinances such as the New York City Administrative Code.

PART: The courtroom in which a judge presides over cases.

PART F Felony: Cases fall under the jurisdiction of Criminal Court until a Grand Jury indictment is obtained. After arraignment in Criminal Court, felony cases in New York County are adjourned to a Criminal Court All Purpose Part called Part F. After a Grand Jury indictment has been voted, the case moves to a Supreme Court Arraignment Part.

PLEAS: Dispositions in which the prosecutor and defendant agree on a particular charge to which the defendant will plead guilty. Most often, pleas will have a sentencing recommendation. A judge must approve the plea.

PRECINCT: The City of New York is divided into smaller sections, which are patrolled by units of the police department. Each precinct has a station-house. Manhattan has 22 precincts.

PROBATION DEPARTMENT: The department responsible for the supervision of persons placed on probation in lieu of imprisonment. This department also conducts pre-sentence investigations used by judges when determining sentences.

RELEASED ON OWN RECOGNIZANCE (ROR): When the court determines that a defendant is likely to appear in court as required by law, bail may be deemed unnecessary and the defendant is released without posting bail.

REMAND: In serious cases when the court determines that a defendant is likely to flee the jurisdiction of the court, the court may determine that bail should not be offered. Remanded defendants remain in custody.

ROSARIO: Rosario material includes any statements of a witness who will testify at trial. Police forms that summarize a witness' statement, a signed statement by a witness, and paperwork prepared by a testifying police officer are examples of Rosario materials. Rosario material must be given to the defence before the opening statements.

STENOGRAPHER OR COURT REPORTER: Takes verbatim record of court proceedings using a stenotype machine which records stenographic symbols on paper.

SUPREME COURT: In New York State, the court in which felonies are tried. Though the name is misleading, the Supreme Court of New York is not the highest court in the state--the Court of Appeals is the highest court in New York State.

SUPREME COURT CALENDAR PART: The Supreme Court Calendar Part is the part in which various proceedings occur between Supreme Court arraignment and trial. Motions and pleas are handled in the Part.

TRIAL: A criminal trial is a formal examination of evidence before a court of law or a jury to determine whether a defendant is guilty of the charges brought against him beyond a reasonable doubt.

TRIAL COURT PART: The court part in which trials occur.

UNCONDITIONAL DISCHARGE: A sentence of an unconditional discharge is imposed when the judge believes that no proper purpose would be served by imposing any conditions on the defendant.

VIOLATION: An offence carrying the lowest sanctions. Although they are penal in nature, violations are not defined as crimes. The maximum term of imprisonment is 15 days.

VOIR DIRE: Voir Dire is the name given to jury selection. In Criminal Court, 6 jurors and 1 or 2 alternates are chosen. In Supreme Court, 12 jurors and 2 to 4 alternates are chosen. When prospective jurors are brought to the courtroom, the judge will explain certain principles of law and question the prospective jurors. The ADA then questions the jurors. After the ADA has finished, the defence attorney asks further questions. Outside of the presence of the jury and following established rules, the attorneys will excuse jurors they believe should not sit on the case. The remaining jurors are sworn in. The process continues until the full number of jurors and alternates is chosen.

WARRANT: A judicial writ authorizing an officer to execute a search, seizure, or arrest.

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H. & Nunamaker, J.F. (2010). Detecting fake websites: the contribution of statistical learning theory. *MIS Quarterly, 43,* 435-461.

Adcox, S., (2002). "Authorities in New York Nab Ring at Center of Largest-Ever Identity-Theft Case." *Albany Times Union.*_Highbeam Research: http//www.highbeam.com/doc1G1-94875562.html.

Aggarwal, S., Duan, Z., Jones, F. & Liu, W. (2010). Trust-based Internet accountability: Requirements and legal ramifications. *Journal of Internet Law, April,* 3-16.

Akers, R.L. (1997) *Criminological Theories: Introduction and Evaluation.* Los Angeles, CA: Roxbury.

Al Harby, F., Qahwaji, R & Kamala, M. (2010). Towards an understanding of user acceptance to use biometrics authentication systems in e-commerce: using an extension of the technology acceptance model. *International Journal of E-Business Research, 6,* 34-55. DOI: 4018.jebr.2010070103

Principles of Professional Responsibility. Adopted by the Council of the American Anthropological Association May 1971. *American Anthropologist* 51:370 (1949)

Bennett C. 2010. *NYPD officers face stat fudging* [Online]. Available at http://www.nypost.com/p/news/local/nypd_officers_face_stat_fudging_YbjR8bHLCv70t1H746nFmK#ixzz27AmNfbwE [Assessed: 15 October 2010].

Bauer, J. (2010, January 5). Identity Theft: Trends and Issues. In *www.crs.gov*. Retrieved December 25, 2011.

Berg, S.E. (2006). Recommendations for a comprehensive identity theft victimization survey framework and information technology prevention strategies. Rochester Institute of Technology, April 7, http://www.sparsa.org/res/research/IDTheftVictim.pdf, 1-85.

Bergholz., A., de Beer, J., Glahn, S., Moens, M.F., Paas, G. & Strobel, S. (2010). New filtering approaches for phishing email. *Journal of Computer Security, 18,* 7-35. DOI:10.3233/JCS-2010-0371 Boetig, B.P. (2006). The routine activity theory: a model for addressing specific crime issues.

Conradt, C. - *Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case*2011 *International Journal of Cyber Criminology* (IJCC) ISSN: 0974 – 2891 January – June 2012, Vol 6 (1): 912–923.

FBI Law Enforcement Bulletin, 12-20.

Bose, I. & Leung, A.C. (2009). What drives the adoption of anti-phishing measures by Hong Kong banks? *Communications of the ACM, August,* 141-145. DOI:10.1145/1536616.1536643.

Bronk, C. (2008). Hacking the nation-state: security, information technology and polices of assurance. Information Security Journal: a global perspective, 17, 132-142. DOI: 10.1080/19393550802178565.

Burdon, M. (2011). Contextualizing the tensions and weaknesses of information privacy and data breach notification laws. Santa Clara Computer & High Tech Law Journal, 27, 63-130.

Campbell, D.T., & Stanley, J.C. (1996). *Experimental and Quasi-Experimental Designs for Research.* Chicago, IL. :Rand-McNally.

Clapper, D.L. (2010). Stolen data and fraud: the Hannaford brothers data breach. *Journal of the* International Academy for Case Studies, 16, 115-129.

Coats, B. (2008). Public information theft. *Quill,* 21-24. *Christine Conradt - Online Auction Fraud and Criminological Theories: The Adrian Ghighina Case*2011 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891 January – June 2012, Vol 6 (1): 912–923.

Computerworld. (2005). Data thefts prompting IT security checks. *Computerworld, March 21,* 10.

Copes, H. & Vieraitis, L. (2007). Identity theft: Assessing offenders' strategies and perceptions of risk. University of Alabama at Birmingham, AL, http://www.search.org/files/pdf/IdentityThievesProfiled.pdf, 1-88.

Cromwell, P., Alexander, G. & Dotson, P. (2008). Crime and incivilities in libraries: situational crime prevention strategies for thwarting biblio-bandits and problem patrons. *Security* Journal, 21, 147-158.

Curtis, C.E. (2011). Rallying round the red flags. *CFO, March,* 14.

Dazeley, R., J. Yearwood, et al. (2010). Consensus Clustering and Supervised Classification for Profiling Phishing Emails in Internet Commerce Security. *Knowledge Management and Acquisition for Smart Systems and Services.* B.-H. Kang and D. Richards, Springer Berlin / Heidelberg. 6232: 235-246.

Denzin, N. K., & Lincoln, Y.S. (Eds.), (1994). *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage.

Devarakonda, A. K., P. Tummala, et al. (2010). Security Solutions to the Phishing: TransactionsBased on Security Questions and Image. *Information Processing and Management*. V. V. Das, R. Vijayakumar, N. C. Debnath et al, Springer Berlin Heidelberg. 70: 565-567.

Domonell, K. (2011). Thwarting ID thieves: what most colleges and universities aren't doing to avoid identity theft and fraud—but should be. *University Business, 14,* 82-88.

Dunham, J., Eck, J.E. & Sampson, R. (2010). Super controllers and crime prevention: a routine activity explanation of crime prevention success and failure. *Security Journal, 23,* 37-53. DOI: http://dx.doi.org/10.1057/sj.2009.17

Dunn, S.E. (2011). Reporting requirements incident to breaches of personally identifiable information. TJAGLCS Practice Notes, *The Army Lawyer, April,* 37-38.

DVM. (2009). FTC delays red flags rule enforcement. *DVM Newsmagazine; June,* 12-14.

Ellison, N. (2007). Facebook Use on Campus: A Social Capital Perspective on Social Network Sites. *Paper presented at the ECAR Symposium, Boca Raton, FL.* December 5-7, 2007. Retrieved from http://www.educause.edu/ecar.

Farrell, G., Tilley, N., Tseloni, A. & Mailley, J. (2010). Explaining and sustaining the crime drop: clarifying the role of opportunity-related theories. *Crime Prevention and Community Safety, 12,* 24-41. DOI:10.1057/cpcs.2009.20.

Federal Trade Commission. (2010). Overview of the Identity Theft Program, October 1998-*September 2003*. http://www.ftc.gov/os/2010/09/timelinereport.pdf

Fell, B.D. (2006). Identity theft and routine activities: a test of victimization using college students. Louisville, Kentucky, Department of Justice Administration, http://digital.library.louisville.edu/utils/getfile/collection/etd/id/672/filename/673.pdf, 1-84.

Ferguson, A. J., Fostering e-mail security awareness: *The West Point carronade. Educause Quarterly*, 28(1), 2005.

Fernandez, C. (2010). Chip and Pin Flaw that banks tried to censor: Cambridge Scientist exposed security failures. *Mail Online, December 2010.* http://www.daily ail.co.uk/news/article- 1342218.

Financial Crimes Enforcement Network Identity Theft Trends, Patterns, and Typologies Based on Suspicious Activity Reports Filed by the Securities and Futures Industries January 1, 2005 – December 31, 2010.
http://www.fincen.gov/news_room/rp/files/ID%20Theft%2011_508%20FINAL pdf - 2011-September.

Findings in Javelin Strategy and research cited in Worthen, Ben. (2009). "Card holders Buy Peace of Mind, If Not Security," *The Wall Street Journal*, March 10, 2009. D1.

Fogel, J. & Nehmad, E. (2008). *Internet Social Networking Communities: Risk Taking, Trust, and Privacy Concerns.* Computers in Human Behavior, 25, 153-160.

Fox, J. L. & Lundman, R. “Problems and Strategies in Gaining Research Access in Police Organizations” *Criminology: An Interdisciplinary Journal.* P.53. vol. 12, no. 1, May, 1974.

Frank, M. J., and Associates. (1998). Identity Theft Prevention and Survival: Identity Theft and Assumption Deterrence Act of 1998, www.identitytheft.org.

Garrie, D.B., Griver, Y. & Joller, M. (2010). Regulating spyware: challenges and solutions. Journal of Internet Law, February, 3-14.

Giles, J. (2010). History of social network use makes you easier to identify online. *New Scientist, 206,* 1- 2.

Glithero, K. (2009). Picking numbers out of thin air: federal aggravated identity theft prosecutions in light of Flores-Figueroa. *American Journal of Criminological Law, 37,* 69-96.

Graybook (2011). New York Criminal Statutes and Rule.

Greenwood, B. (2009). Stolen laptop leads police to identity theft ring. *Information Today,* September, 44.

Groff, E.R. (2008). Adding temporal and spatial aspects of routine activities: a further test of routine activity theory. *Security Journal, 21,* 95-116. DOI:10.1057/palgrave.sj.8350070

Hayward, K. (2007). Situational crime prevention and its discontents: Rational Choice Theory versus the “culture of now.” *Social Policy & Administration, 41*(3), 232 – 250.

Holtfreter, K., Piquero, N. L., & Piquero, A. R. (2008). And justice for all? Investigators’ perceptions of punishment for fraud perpetrators. *Crime, Law and Social Change, 49*(5), 397 – 412.

Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimization: who gets caught in the net? Current Issues in Criminal Justice, 20, http://www98.griffith.edu.au/dspace/bitstream/handle/10072/28075/55533_1.pdf?sequence=1, 1-20.

Information Week. (2009). Laptop theft nets data on 800,0000 doctors. *Information Week,* October 15, 1- 2.

Information Week. (2009). Internet has never been more dangerous. *Information Week,* September 30, 1-2.

Information Week. (2009). Identity theft malware surges 600%. *Information Week, August 19,* 1-2.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., & Menczer, F. (2007, October). *Social phishing.* Communications of the ACM, 50(10), 94-100.

Jefson, C.A. (2007). Identity theft and consumer health education: case study teaching the skill of decision making. *Journal of School Health, 77,* 373-386.

Kunick, J.M. & Posner, N.B. (2011). Following the red flag rules to detect and prevent identity theft. Information Management, May, 25-29.

Lee, G. (2009). Raising red flags: a primer on new regulations regarding identity theft prevention. *PT in Motion, 1,* 48-52.

Levi, M., Burrows,John (2008*).* Measuring the Impact of Fraud in the UK: A Conceptual and Empirical Journey. *British Journal of Criminology* Volume:48 Issue:3, 293-318

Liebowiz, J. (2012). Prepared statement of the Federal Trade Commission before the committee on Commerce, Science and Transportation, United States Senate; on The Need For Privacy Protections: *Perspectives from the administration and the Federal Trade Commission.* http://search.ftc.gov/search?utf8=%E2%9C%93&affiliate=federaltradecommission&query=cite+for+ftc&commit=Search Retrieved on September 21, 2012.

Listerman, R.A. & Romesberg, J. (2009). Are we safe yet? *Strategic Finance, July,* 27-34.

Luo, X. & Liao, Q. (2007). *Awareness education as the key to ransomware prevention.* Information Systems Security, 16, 195-202.

Malinowski, B. (1961). *Argonauts of the Western Pacific.* New York: Dutton

Mansfield-Devine, S. (2008, November). *Anti-social networking: Exploiting the trusting environment of Web 2.0.* Network Security, 4-7.

Manz, W. H., (2003). Federal Identity Theft law; Major Enactments of the 108th 1 & 2.

McKee, L J.B. & McKee, T.E. (2011). Helping taxpayers who are victims of identity theft. *The* CPA Journal, 81, 46-55.

McMillion, R. (2009). Taking aim at red flags. *ABA Journal, 95,* 1-3.

Mensch, S. & Wilkie, L.A. (2011). Information security activities of college students: an exploratory study. Academy of Information and Management Sciences Journal, 14, 91-119.

Meithei, T.D. & Sousa, W.H. (2010). Carjacking and its consequences: a situational analysis of risk factors for differential outcomes. *Security Journal, 23,* 241-258. DOI;10.1057/sj.2008.19

Miyamoto, D., Hazeyama, H. & Kadobayashi, Y. (2010). HumanBoost: utilization of users' past trust decision for identifying fraudulent websites. *Journal of Intelligent Learning Systems and Applications, 2,* 190-199. DOI:10.4236/jilsa.2010.24022.

Moore, A. P., (2004). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance *Center*. U.S. Secret Service and CERT Coordination Center.

Murdoch, S.J., Drimer, S., Anderson, r., and Bond, M. (2010) . Chip and Pin is Broken. http://www. Test.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf.

Nicho, M. & Fakhry, H. (2011). An integrated security governance framework for effective PCI DSS implementation. International Journal of Information Security and Privacy, 5, 50-67.

Otto, P.N. (2009). Reasonableness meets requirements: regulating security and privacy in software. Duke Law Journal, 59, 309-343.

Owen, K., Keats, G., & Gill, M. (2006) The Fight against Identity Fraud: A Brief Study of the EU, the UK, France, Germany, and the Netherlands. *The Police Chief,* vol. 74, no. 5, May 2007.

Pascoe, T., Owen, K., Keats, G., and Gill, M. (2006). *Identity Fraud: What about the Victim? CIFAS*, Perpetuity Research & Consultancy International Ltd, United Kingdom.

Ramsey, G. & Venkatesan, S. (2010). Cybercrime strategy for social networking and other online platforms. *The Licensing Journal,* 23-28.

Randazzo, Marisa Reddy, Michelle M. Keeney, Eileen F. Kowalski, Dawn M. Cappeli, and Reyns, B.W. (2010). A situational crime prevention approach to cyberstalking: preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety, 12,* 99-120. DOI: http://dx.doi.org/10.1057/cpcs.2009.22

Rubens, J.T. (2009). So many privacy rules! The developing standard of care for data security and identity theft protection. *Business Law Today, 18,* 55-62.

Saad, L. (2009). Two in three Americans worry about identity theft. *Gallup Poll News Service, October* 16, 1-2.

Smith, M.J. (2009). A six-step model of potential victims' decisions to change location. *Security Journal, 22,* 230-249. DOI:10.1057/sj.2009.6.

Stevens, G. (2012). Legislative Attorney gstevens@crs.loc.gov, 7-2581 *Congressional research service.* P. 151 March, 2012.

Sullivan, R.J. (2010). The changing nature of U.S. card payment fraud: industry and public policy options. *Economic Review, 95,* 101-126.

Tillyer, M.S. & Kennedy, D.M. (2008). Locating focused deterrence approaches within a situational crime prevention framework. *Crime Prevention and Community Safety, 10,* 75-84. DOI: 10.1057/cpcs.2008.5

Ruderman, W. 2012. New York Police Department manipulates crime reports. *New York Times.* 29 June 2012. NY region.

Tomescu, M. & Trofin, L. (2010). Identity, security and privacy in the information society. Contemporary Readings in Law and Social Justice, 2, 307-312.

U.S. Government Accounting Office, "Identity Fraud," p. 40, Report No. GGD-98-100BR, (1998).

U.S. Department of Justice Programs Bureau of Justice Statistics Crime Data Brief November 2011 "Identity Theft Reported by Households, 2005-20010" by Lynn Langton, *BJS Statistician.* http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh0510.pdf - 2011-November

Van Maanen, J., Dabbs, J. M., Faulkner, R. R. (1982). *Organization; Psychology; Research.* Beverly Hills: Sage.

Verma, A. (2007). Anatomy of riots: a situational crime prevention approach. *Crime Prevention and Community Safety, 9,* 201-221. DOI: 10.1057/palgrave.cpcs.81590044

Visa Inc (2011). Press release. Accelerate Chip Migration and Adoption of Mobile Payments. http://corporate.visa.com/media-center/press-releases/press1142.jsp.

Wagner, C.G. (2009). Internet fraud on the rise. *The Futurist, July,* 15. http://www.financialfraudaction.org.uk/Publications/#/58/

Wartenberg, D. & Thompson, D. (2010). Privacy versus public health: the impact of current confidentiality rules. American Journal of Public Health, 100, 407-414.

Weekly Compilization of Presidential Documents. (1998). Vol. 34 Legislative History—H.R. 1731 (S. 153): House Reports: No. 108–528 (Comm. on the Judiciary). *Congressioanl Record*, Vol. 150 (2004)

Winn, J.K. (2010). Are better security breach notification laws possible? *Berkeley Technology* Law Journal, 24, 1133-1167.

Wortley, R. and Mazerolle, L. (2008). *Environmental Criminology and Crime Analysis.* Cullompton, UK: Willan Publishing.

Zaharia, G.C., Zaharia, C., Tudorescu, N. & Zaharia, I. (2010). Online crime and the regulation of business on the Internet. Economics, Management and Financial Markets, 5, 238-245.

Using FACTA Remedies: An FTC Staff Report on a Survey of Identity Theft Victims www.ftc.gov/os/2012/03/factareport.pdf.