CHOOSING IDENTITY THEFT: IMPULSIVITY OR RATIONAL CHOICE?

Samuel Haycraft IV

A Thesis Submitted to the
University of North Carolina Wilmington in Partial Fulfillment
of the Requirements for the Degree of
Masters of Arts

Department of Sociology and Criminology
University of North Carolina Wilmington

2013

Approved By

Advisory Committee

Michael Maume

Randy LaGrange

Babette Boyd

Cecil Willis

Chair

Accepted By

Dean, Graduate School
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Start Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABSTRACT</td>
<td>iv</td>
</tr>
<tr>
<td>ACKNOWLEDGEMENTS</td>
<td>v</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>1</td>
</tr>
<tr>
<td>Statement of problem</td>
<td>2</td>
</tr>
<tr>
<td>Purpose of research</td>
<td>5</td>
</tr>
<tr>
<td>Research on identity theft</td>
<td>6</td>
</tr>
<tr>
<td>RATIONAL CHOICE THEORY</td>
<td>13</td>
</tr>
<tr>
<td>Bounded rationality</td>
<td>16</td>
</tr>
<tr>
<td>SELF-CONTROL THEORY</td>
<td>17</td>
</tr>
<tr>
<td>RESEARCH DESIGN AND METHODS</td>
<td>19</td>
</tr>
<tr>
<td>Origin of secondary data</td>
<td>19</td>
</tr>
<tr>
<td>Descriptive characteristics of sample</td>
<td>20</td>
</tr>
<tr>
<td>Qualitative research</td>
<td>21</td>
</tr>
<tr>
<td>Qualitative data analysis software</td>
<td>22</td>
</tr>
<tr>
<td>Analysis strategy</td>
<td>22</td>
</tr>
<tr>
<td>RESEARCH FINDINGS</td>
<td>23</td>
</tr>
<tr>
<td>Working in groups</td>
<td>24</td>
</tr>
<tr>
<td>Prior criminal history</td>
<td>25</td>
</tr>
<tr>
<td>White-collar crime</td>
<td>25</td>
</tr>
<tr>
<td>Motivations</td>
<td>26</td>
</tr>
<tr>
<td>Ease of crime</td>
<td>26</td>
</tr>
<tr>
<td>Money</td>
<td>27</td>
</tr>
<tr>
<td>Risks</td>
<td>29</td>
</tr>
<tr>
<td>Ignorance about the crime</td>
<td>29</td>
</tr>
<tr>
<td>Preventative measures taken</td>
<td>30</td>
</tr>
</tbody>
</table>
ABSTRACT

Identity theft is one of the fastest growing segments of crime in the United States in recent years. Computer access to personally identifying information has made this a lucrative crime that is relatively easy to accomplish with limited skills. This study examines and identifies the factors involved in the decision-making process to commit identity theft. Secondary data gathered from Copes and Vieraitis (2007) is analyzed qualitatively through the use of MaxQDA to find potential patterns amongst offenders. The analysis is done through the use of two theories, primarily rational choice theory, with self-control theory being supplemental to analyze possible impulsivity. Several factors were found including drug usage, addictive behavior and lifestyles, and ease of accomplishment of the crime that influenced the decision-making process. The research findings show a need for policy changes to increase the risk of this crime and limit exposure of identifying information being maintained by organizations and institutions. Further research is needed to gain insight into offender mindsets and create an understanding of the typical identity thief.
ACKNOWLEDGEMENTS

My sincerest thank you goes to my committee members who worked with me throughout the entire year through the learning curve of conducting this research. My committee chair, Dr. Cecil Willis, was a great help along the way and an irreplaceable part of this research. He worked relentlessly to help perfect the work being produced. Thank you for helping hone in the theories to be utilized and helping me throughout my years at UNCW to gain a better theoretical understanding in criminology. Dr. Randy LaGrange deserves many thanks for helping me to keep calm throughout the struggles that I encountered during the course of the research. Dr. LaGrange was actually the reason I became a criminal justice major in my undergraduate studies at UNCW. Little did I know then that I would go on to obtain a Masters degree from the same department. Dr. Michael Maume helped guide the overall basis of the research and helped obtain the data that was utilized and I thank him for his patience throughout this academic journey. Thank you for all you have taught me in the field of data analysis. Professor Babette Boyd I sincerely appreciate your guidance along the way of this research and for guiding me onto the academic path I am on today. Were it not for your mentoring and positivism I would not be attending law school this fall. To all of my committee members, it has been a great pleasure working with you all through my tenure as a student of this department, both in undergraduate and graduate studies.

To graduate school friends, you have all become like a family to me and I fully believe we all made it through this together because we were there for each other day in and day out. It is hard to believe it has already been two years and that our time has come to an end as graduate students at UNCW. I’d also like to thank my mother, father, and sister for being there throughout the entire process as well.
INTRODUCTION

Overview

Identity theft is a crime designed to steal one’s credit or identifying financial information to gain access to finances for the purchase of goods or to defraud. Typically one will not realize their identifying information is being stolen. Even though it is not a victimless crime, it does usually occur off the street by highly knowledgeable individuals. According to the Federal Trade Commission (FTC), “Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes,” (Federal Trade Commission, November 14, 2012, 1). The United States Code defines identity theft under U.S. Code Title 18, Part 1, Chapter 47, Section 1028 (18 U.S.C. § 1028). The Identity Theft Assumption and Deterrence Act of 1998, states,

“Whoever, in a circumstance described in subsection (c) of this section—knowingly transfers,possesses,or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law,” (18 U.S.C. § 1028). 1

The Bureau of Justice Statistics tracks identity theft reports by household in the United States through victims self-reporting. A longitudinal study was conducted on data from 2005 to 2010, with 2008 data being excluded due to data only being collected for a six-month period. A trend was noted from 2005 data through 2009 data, with identity theft reports rising. The types

---

1 A complete definition of all subsections of 18 U.S.C. § 1028 is provided in Appendix A.
2 A complete definition of all subsections of 18 U.S.C. § 1028A is provided in Appendix B.
of identity theft reported were categorized as existing credit card accounts, other existing
accounts, personal information, and multiple types of victimization. From 2005 to 2009, all
categories saw a rise in reporting; while in 2010, numbers decreased slightly for all categories.
There was an increase of 50 percent in misuse and attempted misuse of existing credit card
accounts from 2005 to 2010.

Statement of problem

This research explores the factors that contribute to decisions to commit identity theft.
Are there common factors that could be used to raise flags to authorities before there are victims
that suffer at the hands of these criminals? Surely the targets of identity theft are affected, but
identity theft holds lasting effects for most people due to the financial loss and potential credit
problems. The research expands on Copes and Vieraitis’ (2007) original study through the
introduction of self-control theory as an explanation of an offender’s actions.

Identity theft damages credit history, which means it could take years for a victim to be
credit-worthy again if the issue is not resolved with crediting agencies. When one conjures the
thought of theft it creates a thought of a physical item being stolen, but that’s not always the case
with identities. Thieves could steal physical credit cards from a person, but that would alert the
victim, hence prohibiting any major length of time for the thief to make purchases. This crime is
about the theft of “imaginary money;” granted the money does exist, but not in a physical form
for every dollar stored in banks in the world. Therefore, society has taken to creating money as
0’s and 1’s through the use of electronic banking. The Internet has allowed for an avenue for
identities to be compromised by a person simply gathering the appropriate information on
someone they wish to victimize. This victimization could be accomplished by making shopping
purchases online, hacking into a bank account and transferring funds, or even filling out credit
card applications in someone else’s name, typically the name of the identity they’ve stolen. Identity theft does not even have to involve the stealing of money, although it typically does. Over 5% of households in the United States, which is approximately 6.4 million homes, reported someone in the home had been victimized by identity theft in the last six months, according to the National Crime Victimization Survey (NCVS). (Copes and Vieraitis, 2009a:239) Obviously the NCVS is not a foolproof gauge on how widespread the problem is, as not all victims will be interviewed and even those who have been victimized are not guaranteed to admit it. However, it is a well-respected resource to understand the prevalence of crimes that are under reported to law enforcement.

Due to the increases in the past ten years in identity theft, many different policies have been instituted to help victims limit the potential lasting effects. Fraud alert systems have been put in place for the three major credit bureaus, which will keep a closer watch on individuals who place alerts on their accounts to detect fraud. Policies were put into place to allow consumers to request a free credit report from each of the three major bureaus once a year. Merchants can only list a maximum of the last five digits of a credit card on a purchase receipt. Mandatory sentencing guidelines for convicted offenders were established. (Copes and Vieraitis, 2009a)

Typically economic crimes are classified as white-collar crimes due to the nature of the offense. However, sometimes, white-collar cases are defined by characteristics of the perpetrator. In the case of identity theft neither of the previously described criteria allows for a justified fit within the classification of white-collar crime. Identity thieves come from all kinds of backgrounds, although in the Copes and Vieraitis (2007) data set that will be utilized, most
offenders are from middle-class backgrounds. Copes and Vieraitis (2009b) examine where identity theft should fall in classifications of white-collar versus blue-collar crimes:

“According to Braithwaite (1985), the most influential partition has been Clinard and Quinney’s (1973) separation of white-collar crime into occupational and corporate crime. In doing so, the term corporate crime preserves the original definition of white-collar crime as delineated by Sutherland, but recognizes that lower level white-collar and even blue-collar workers commit crimes in the context of their occupations. Others have added forms of government crime, hybrid forms of white-collar crime (e.g., state-corporate crime crimes of globalization, and finance crime), and “residual” forms such as technocrimen and avocational crime (Friedrichs, 2004),” (2009b:330).

There are two stereotypes of identity thieves found throughout research and literature. Those two types are either drug users who are strung out looking for a quick way to make some cash, or a highly intelligent, sophisticated person intent on gaining large sums of money. Due to the nature of the crime, most of these offenders are not apprehended, as clearance rates amongst law enforcement for this crime are incredibly low, with estimates as low as 10%. (Copes and Vieraitis, 2009c:566) So therefore, we may not be able to properly categorize this crime because we do not know enough about all the offenders of this nature. We can theorize based on the offenders that have been arrested and convicted, but it would seem as though those individuals would be the tip of the iceberg. Due to low clearance rates and the difficulty of tracing offenders, it is possible that identity theft will not be fully understood from an offender perspective for years to come.

A recent publication has even highlighted social network profiles being utilized to compromise as a form of identity theft. ProtectMyID.com, an organization run by credit bureau giant Experian, published an article in 2010 uncovering the trend of thieves creating fake social network profiles to pose as someone and gain access to that person’s friends to target them for identity theft. “…many privacy experts note that because these websites are built around self-selected networks of friends or colleagues, people using them may be more trusting of
communications they receive through the sites—thereby putting themselves at greater risk of getting scammed.” (ProtectMyID.com, 2010) Cliché scams, such as a long lost relative seeking monetary support, which used to be conducted through emails, are now making their way to social networking sites, such as pleas for money being wired to help a friend in need. Even malware is being delivered through social networking in an attempt to gain access to information from financial institution websites one visits on their personal computer.

Purpose of research

The purpose of this research is to explore the factors that contribute to identity thieves’ decision-making process. This research will be based on secondary analysis of qualitative data gathered through interviews with inmates incarcerated for the crime of identity theft. The research question is “What are the common factors involved in the decision-making process of identity thieves’ choice to commit the crime?” The research results will be analyzed through the theories of rational choice and self-control to determine which theory has better applicability to explain the actions of identity thieves. The intent is to offer possible solutions to prevent identity theft in the future.

The following sections include a review of previous research on identity theft, discussions of rational choice theory and self-control theory, the research design and methods for this thesis, research findings, conclusions and finally future implications for research and policies. The literature review and theoretical sections will inform the formulation of hypotheses and factors to be included in the analysis. The operationalization of these factors is dependent on the variables in the dataset.
This thesis research is based on data previously gathered by Heith Copes and Lynne Vieraitis (2007), who discovered that the sample of identity thieves they interviewed was quite diverse. Copes and Vieraitis’ methods included assessing the crime of identity theft from the offender perspective by interviewing 65 offenders housed in federal prisons in each of the six Federal Bureau of Prisons regions in the United States. Inmates for the sample were found through the use of LexisNexis databases for articles regarding convictions and the United States Attorney’s office’s website. The U.S. Attorney’s website was utilized to locate offenders charged with, indicted, and/or sentenced for crimes of identity theft. The search created a list of 470 potential inmates, which was narrowed down to include 297 that were currently being housed across 14 federal prisons. Of the original 65 offenders, the sample was decreased to 59 respondents in Copes and Vieraitis’ complete research because six individuals denied participation or knowledge of identity theft or the six were excluded because of crimes of fraud not including theft of the victims’ identities. Semi-structured interviews were recorded by Copes and Vieraitis, which were later transcribed verbatim. However, due to prison official complications or a subject’s objection, nine interviews were not recorded during the research. The offenders were from both middle-class and working-class backgrounds. Some were leading what society would deem ordinary lives on the surface, while others within the group of thieves led the stereotypical lifestyle of a persistent street offender. The majority of the offenders interviewed were primarily motivated by the need for quick access to money.

Their research points to offenders utilizing cost-benefit analysis to determine the overall risks associated with the crime. Rational choice theory is fully applicable in this situation as the offenders are gauging their perceptions of risk versus the gains associated with the quick cash.
Copes and Vieraitis (2007) found that most identity information was purchased or stolen from others the offender knew, or even stolen out of victim’s mailboxes and trash. These offenders apparently developed skill sets designed to make their tasks easier for them, ranging from social skills to technical skills. However, Copes and Vieraitis found situational awareness and crime prevention techniques to be effective means for limiting the opportunities of crime. Although the authors noted that offenders find new ways to adapt to the ever-changing field of information technology and identity protection in order to achieve their goal.

Copes and Vieraitis (2007) found that the majority of the offenders had been previously arrested for crimes including identity theft, fraud, drug use and distribution, as well as property crimes. Most identity thieves do not think about getting caught, much like other criminals, yet typically when the offenders do think about the risks associated with their actions, they neutralize and minimize them so much that the benefits are outweighing the risks of the act. As suggested previously, these thieves could be blue-collar workers or white-collar office workers. Copes and Vieraitis found that approximately one-third of the individuals interviewed utilized their job position to take control of their victim’s identity. They found that these employees were mortgage officers, government agents, or even run-of-the-mill business workers in banks, universities, and other locations that have access to information that could be used to steal one’s identity. The authors noted some of the motivations for the theft were using the information to produce other documents such as driver’s licenses, create fake checks, apply for new credit cards, and loans with the stolen identity.

Copes and Vieraitis (2007) offered recommendations for decreasing the prevalence of this crime. Among those recommendations was increasing the effort and risks that come with obtaining the information that is used to gain access to cash or other goods. Some of the
specifics were to control access to mailboxes and trash, observe better practices for document disposal, limit access to sensitive information, and develop better practices for identification requirements when accessing information that should be secured.

Copes and Vieraitis certainly lead the field in identity theft research from the perspective of the offenders, but several others have examined this growing phenomenon in criminality. Michael Benson challenged the idea that identity theft is a new form of crime with his contention that imposters have been around for a while; they just have a new form of acquisition. He noted, “Pretending to be someone else or using someone else’s personal information to facilitate illegal activities is a technique that has been around for some time. It was not just recently invented. Yet in the 1990s, this technique became a lot easier and a lot more lucrative to use,” (2009:231).

Technological advancements played a major role in the increase of identity theft due to how readily available information was in a centralized location, namely the Internet. Furthermore, financial regulations were relaxed allowing individuals to create lines of credit, which caused criminals to see the advantage of stealing someone else’s information due to its potential value in financial services. Identity theft is a fast growing segment of criminality that has estimates of up to 10 million occurrences a year (White and Fisher, 2008:3). With estimates that high, it’s no wonder that Americans raised many alarms in attempts to secure the vital information that was so easily accessible to prying hands.

Due to the increased attention from this newly popular crime, state and federal officials began creating new statutes that specifically targeted identity thieves. Never before was this crime so prevalent, hence there were not appropriate penalties associated with the act. However, like any other crime, once it gains enough public interest, the government addresses it in an attempt to limit its prevalence in society. Although simply passing legislation will not prevent a
crime, there must be some type of situational and environmental preventions. If that were the case, there would be no criminals in the United States as there are laws created to punish offenders of acts deemed illegal, such as murder, rape, and many others. There are other ways to prevent a crime, first and foremost of which is protecting your own identity. There are services available to monitor credit ratings and history for suspicious activity. Many people are now more careful about destroying documents with identifying information. Other precautionary actions are also being taken against possible identity theft. Many of the criminals that were interviewed for Copes and Vieraitis’s research were unaware that there could be severe penalties brought against them for their acts. They assumed they would fall under the umbrella of white-collar crime, which they viewed as less severe and typically given shorter sentences than street crimes.

As with any crime, there are varying opinions on how to handle the response to the growth of its occurrence. Some researchers say that educating the offenders is the proper response while others say that it is the victim’s job to make the theft more difficult to accomplish. In the end, all would agree that there must be action taken against identity thieves due to this largely credit-based world we live in. Graeme R. Newman (2009) wrote in response to arguments put forth in Copes and Vieraitis’s research on thoughts of rationality that will be discussed later in this research. Newman’s biggest issue is that Copes and Vieraitis focus on psychological aspects of the crime instead of physical attributes such as how the crime was committed and the techniques utilized. However, due to such a wide band of possibilities amongst identity thieves, it is less important as to how the offenders carried out the crime and more important for potential victims to learn the logic behind the process, in hopes of limiting exposure to such criminals. If enough individuals can limit their exposure to victimization, it is
likely there would be fewer opportunities for these criminal activities. One can avoid being a victim by protecting identifying information and limiting their exposure to potential thieves.

Yet, some people even find themselves pondering the rubric of an identity theft crime. Identity theft, as previously noted, can encompass numerous avenues of actions taken to obtain information. Newman (2009) notes the difficulty in defining identity theft due to a broad range of techniques utilized by offenders including credit card fraud, check fraud, and forgery.

Newman notes his ideas on defining identity theft:

“...In fact, as is widely acknowledged, defining identity theft (or fraud) is close to impossible because it is made up of many different techniques that may themselves be crimes, such as credit card fraud, check fraud, counterfeiting, document forgery, impersonation, stalking, mail fraud, and many others (Newman, 2008). So, assessing the extent of identity theft depends considerably on how broadly one defines it.” (2009: 271)

Almost all criminals rationalize their actions to themselves in some form; identity thieves would be no different than other common offenders. Newman discusses the idea of “bounded rationality,” where the rationale of the offender is bound within the scope of positivism. Essentially the offenders are maintaining only positive thoughts about their crime and suppressing negative feelings. These offenders positively rationalize their actions to make themselves feel better about the acts. They convince themselves they are committing a crime for the “right” reasons. However, reality in this world is how we construct it in our own lives. Our realities are shaped by the interactions we have on a daily basis. The social construction of reality at times makes criminals feel as though they are not committing a crime, but rather carrying out a “normal” act that other people just don’t agree with.

“Identity theft falls close to the border between crime and mere inconvenience, which makes it an unlikely issue to surface suddenly as an acute social problem,” stated Henry N. Pontell (2009:265). Obviously identity theft does not come to mind when someone says the
word “criminal,” as you are likely to conjure up images of murders or some other particularly heinous crime. Identity theft is a crime that is difficult to trace, therefore making it harder for law enforcement to make arrests. Technology has just furthered the abilities of these individuals to avoid apprehension.

“Increasingly, criminals today are taking advantage of electronic weapons to steal victims’ identities. They operate offshore, from safe havens, and flood cyberspace with phony requests from legitimate businesses, such as eBay and Chase National Bank, which indicate the need for an ‘update’ on identifying information. The requests often are packaged with the correct logo and letterhead of the firm as well as with a fictitious story about some foul up that will bring an end to the recipients’ access to an account or other resource unless the legitimizing information is immediately forwarded.” (Pontell, 2009:265)

These kinds of “attacks” are calling phishing emails that are sent to users of the particular database that the attackers are attempting to gain access to. This type of scam worked very well in the early days of its use, although in recent years it is less successful as more people are aware of the fictitious emails being sent out to the masses. Yet this is just one example of how criminals are always trying to be one step ahead of the general public to gain leverage over citizens.

Copes and Vieraitis (2009a:238) found that offenders analyze the risks and rewards of each crime in an interpretive manner determining whether or not the risk is an attractive possibility given the rewards. It has been estimated that there is approximately $20 million in financial losses amongst victims of identity theft per year. However due to underreporting it is unclear if this figure is realistic or simply an educated guess based on the number of complaints made to the FTC, the agency appointed to oversee identity theft complaints.

Most identity thieves who get captured do not feel as though they have done anything wrong, or at the very least feel no remorse about their actions. This is due to neutralizing the effects on the psyche. Social bonds have a strong power over humans, yet not necessarily strong
enough to prevent crime. The bonds individuals have with family members, friends, coworkers, and others in their lives typically keep most people on the legal side of the law. Although, there are plenty of people within society who commit crimes and must deal with this internally, while still maintaining all bonds with others. Some neutralize the effects of their crime by associating with other criminals, those who will not look down upon a thief, therefore avoiding shaming. One must neutralize the shaming and guilt associated with their actions in order to justify their actions to themselves and those closest to them. Copes, Vieraitis, and Jochum (2007) brought up an astonishing factor that one would assume enters the thoughts of every criminal, especially a criminal who is stealing all of a person’s wealth and entire identity. In order to continue victimizing others, one must cleanse their conscience.

Identity theft is thought of as a white-collar crime. White-collar crime is defined as “any violations of criminal, civil, or regulatory law—or deviant, harmful or unethical actions—committed during the course of employment in various occupational systems,” (Payne, 2012:652). White-collar criminals are thought of, stereotypically, as upper class, educated members of society. Criminologists and society generally view financial crimes as white-collar crimes. Typically identity theft is a financial crime, certainly in discussions of this particular sample due to their monetary gains from the crime. Brian Payne (2012) wrote a book discussing white-collar crime and its various forms. Within that text, Payne notes several of the types of crimes that the offenders in this study committed, including credit card theft, mortgage fraud, real estate fraud, appraisal fraud, and mail fraud. This is just a sample of the types of crimes that offenders in this sample were prosecuted for under the Identity Theft Assumption and Deterrence Act of 1998, 18 U.S.C. § 1028.
Sometimes offenders are carrying out a crime for the benefits to their lifestyle, typically as a party type of lifestyle. These individuals who commit crimes to support the party lifestyle generally have a blatant disregard for societal norms. “This generally means avoidance of the world of routine work and freedom from being "under someone's thumb””, (Shover and Honaker, 1992:10). In the case of identity thieves, they would be stealing someone’s identity either for monetary gains to support their partying or as an avenue to avoid being caught by authorities. Those who live out the party lifestyle primarily spend their financial gains from their crimes on drugs or alcohol (Shover and Honaker, 1992:10). This party type of lifestyle can lead to carelessness and a lack of planning which can result in the offender being caught.

RATIONAL CHOICE THEORY

Rational choice theory (RCT) is an applicable theory to examine the choices identity thieves make. Rational choice refers to when people make choices based on cost-benefit analysis. Cesare Beccaria, who was a classic criminologist, originally developed what would later be known as rational choice theory in the late 1700s. However, his theory was disregarded until the late 1960s when it reemerged with the help of Gary Becker and James Q. Wilson. In the field of sociology, rational choice theory did not come about until James S. Coleman utilized it in the late 1980s and created a journal devoted to the rationalization of society. Since then, rational choice theory has become quite mainstream in sociology. Rational choice theory is a theory that applies to both an offender specific, as well as offense-specific, crime. That means that for an offender specific crime, the offender takes into consideration their specific skillset and needs prior to committing to a crime. Offense specific crimes are those in which the offender takes into consideration the factors of the actual crime to determine their decisions about carrying out a criminal act. (Siegel, 2008:72)
As previously mentioned, one carries out a crime, as described by this theory, based upon an evaluation of the crime itself and what it will earn the offender. Perhaps the payoff is worth the risk; or perhaps there is some kind of personal vendetta that the offender has and wants to resolve. While total insight into each individual’s thought process when rationalizing their choice in their mind is impossible, this theory appears capable of proving that criminality sometimes simply comes down to self-efficacy and personal discretion. Cornish and Clarke (1985) argued that there are two ways an offender could be involved in a crime, those being criminal involvement and actual criminal events. By criminal events, they literally mean the act of a crime, versus a criminal involvement could be being a conspirator to a crime without actually taking part in the act. Focusing on those with criminal involvement and punishing those actors could potentially limit the opportunities the identity thieves have at their disposal. Perhaps businesses and organizations that do not safeguard the data appropriately should be brought up on charges of criminal involvement due to negligent behavior. While it is acknowledged that this scenario is unlikely to happen, it could with the proper restructuring of laws and regulations. Rational choice theory has had its share of critics. This is why it lost much of its original appeal until the 1960s when it reemerged. Hirschi, Felson, and others from different disciplines, including psychology, challenged the applicability of such a theory. They all, more or less, argued that there were other human nature factors that played into personal crime choices.

“...By Hirschi and by Felson, both of whom believe that rational choice approaches complement rather than supplant existing theory. Hirschi sees rational choice theory as being concerned mainly with explaining crimes (or “events”), in contrast to his “control theory,” which is primarily a theory of criminality (or "involvement"). Felson attempts to provide a synthesis among routine activities, social control, and rational choice perspectives. In his view, rational choice theory deals mainly with the content of decisions; routine activity approaches, in contrast,
are seen to deal with the ecological contexts that supply the range of options from which choices are made,” (Cornish and Clarke, 1985:10).

In the 1960s, the theory came back into the scope of acceptability as more sociologists and criminologists realized its full potential to truly explain one’s actions. Criminologists tend to look at rational choice theory from a criminal standpoint, but the fact of the matter is that people within societies use rational choice theory every day without even realizing it. The human brain is constantly analyzing those costs and benefits while making a decision. Of course there are times where one is more aware of this analyzation, but most of the time it’s done without recollection. Rational choice theory is applicable to the crime of identity theft because offenders are analyzing their chances of getting captured and comparing those probabilities to the overall benefits of the crime. They are rationalizing the illegal act by telling themselves that the gains are substantially worth the risk.

As previously noted in the literature, the identity thieves that were interviewed while incarcerated indicated that they rationalized their decision by downplaying the negative criticisms that arise in one’s mind when feeling guilty about an action. Furthermore, for any criminal, rationalization takes place to inspire them to act out their crime in favor of the gains they will earn. Other theories highlight that part of rational choice is the minimization of pain and the maximizing of pleasure. It certainly is arguable that the convicted offenders interviewed by Copes and Vieraitis, the authors of the research this paper is based off of, gained much pleasure from their crime. The pleasure could have been the monetary gains, the various possessions they acquired, or even the pleasure of successfully stealing someone else’s identity.

Rational choice theory suggests these thieves committed their crimes for the anticipated newfound wealth they expected to acquire in a short amount of time from what they deemed an easy task for earning money. Furthermore, RCT has an element of neutralization where the
offenders must neutralize the psychological effects of the crime in order to suppress the negativity and maximize the pleasure gained from the risks they took.

Bounded rationality

Within rational choice is the idea of bounded rationality, which is when one makes a decision where the rationality of their choice is limited by information available, their cognitive capabilities to process the information, and also the time available to make the decision (Simon, 1997:291). There could be many factors an offender is unaware of during an illegal act, yet some factors are accepted with the risk, such as defense measures that could prevent the offender from accomplishing their goal. It is conceivable to assume that the offenders in this study were acting inside of their own bounds of rationality. The offenders in the sample being studied through the course of this research noted that they were not aware of the consequences of their actions, which could be one logical explanation for their choice as they were operating within the bounds of the situation, unaware of the consequences they could face. Almost all offenders in the sample discussed the notion that they thought the punishment for their act would be based on lack of victims, little to no previous criminal history, and the fact that the crime is a white-collar crime. Those who discussed white-collar crime made note that they feel white-collar criminals get lesser sentencing than violent offenders.

When an offender makes a decision, regardless of how rational they think it is, it will almost always be bounded rationality simply because one cannot know every possible factor that is associated with their decision. Most criminals act within bounded rationality and make choices according to perceptions at the time. Identity thieves are comparable to other criminals, including street criminals (Gottfredson and Hirschi, 1990:200), and therefore would be assumed to making the same kinds of choices without fully understanding the situation. Certainly the
offenders who noted they were on drugs during the theft could not possibly have made fully rational choices; rather they made rational choices in their opinion through the bounds of their perceived rationality.

SELF-CONTROL THEORY

Self-control theory, also known as the general theory of crime (GTC), is a contemporary criminological theory proposed by Michael Gottfredson and Travis Hirschi. The general theory of crime is based on the idea that the reason behind an offender’s crime is a lack of self-control. The general theory of crime (1990) was developed as a new approach to Hirschi’s (1969) earlier theory, control theory of delinquency. Hirschi’s earlier theory focused on society and its institutions, while the new theory went micro-level and focused on the individual and the quality of self-control. GTC acknowledges the widely held conception that one’s propensity to commit crimes decreases as age increases. Closely related, as a person’s age increases throughout childhood up to age ten, the theory assumes an increase in self-control due to various life factors, but once the age of ten is reached self-control should level off and remain stable. Therefore, it is assumed that if one does not have a proper level of self-control in adolescences then that lack of self-control will persist through adulthood. Gottfredson and Hirschi mapped out a list of qualities they expected to observe in an offender. Criminals “tend to be impulsive, insensitive, physical (as opposed to mental), risk-taking, short-sighted, and nonverbal” (Gottfredson and Hirschi, 1990:90). The theorists proposed that if a person did not have these qualities then they had higher self-control, thus being less likely to turn to criminality. Furthermore, if someone had these qualities they were likely looking for instant gratification while acting on a whim. Gottfredson and Hirschi went further into their explanation to refer to someone with these qualities previously listed as a deviant. Obviously society labels criminality
as deviant, therefore one could see that a lack of self-control could cause societal problems, such as identity theft in this particular study. The two authors define crime as “acts of force or fraud undertaken in pursuit of self-interest” (Gottfredson and Hirschi, 1990:15). One’s level of self-control would presumably determine whether the person adheres to societal controls or strays away from expectations. Gottfredson and Hirschi also note that smoking, gambling, and drinking are behaviors that could be linked to criminality, although they mention that a lack of self-control stems from early childhood.

The authors mentioned that they felt that street criminals and white-collar offenders were of the same ideology overall and that they are “likely to share similar characteristics,” (Gottfredson and Hirschi, 1990:200). Essentially the authors were drawing the conclusion that if one does not have self-control, the possibility exists for offenders to cross between street crimes and white collar crime distinctions. In this research it is found that approximately ten percent of the offenders are what would be deemed ordinary street criminals that got into the white-collar business because of their lack of self-control to avoid the impulse to commit identity theft simply based on their mentality of how easy the crime is to commit. However, all the offenders in this research did not act on impulse, rather they meticulously planned their crimes with the hopes of not being captured. One could argue that they were getting involved in identity theft because of a lack of self-control to realize they should not steal other’s personal information, but once they were involved in the crime itself, impulsivity was no longer relevant.

However, it was stated in the theory that a lack of self-control is not a requirement for one to commit a crime, as there are other situational factors and personal reflections that go into the decision-making process (Hirschi and Gottfredson, 1993:53). One could easily argue that an identity thief is shortsighted, seeing only the immediate gains of the crime, insensitive to the
damage the theft will cause, and lacks self-control to refrain from taking something that is not theirs. Identity thieves certainly are seen as deviant, as most people view money and financial information as a treasured and very personal aspect of their lives.

RESEARCH DESIGN AND METHODS

The research question at hand is “How do identity thieves decide to commit their crime? Is it through rational choices or a lack of self-control and impulsiveness?” The hypothesis for this research is that identity thieves generally choose to commit their crime as a result of impulsiveness and a lack of self-control. Hypothesized factors for decision-making utilized by the thieves are lack of protection of information, lack of punishment for offenders, and low clearance rates of the crime by law enforcement. Looking at previous criminal history, drug use, and employment during the crime operationalized these factors. These factors should give some idea as to whether the offender has made a rational decision or if they have acted out of a lack of self-control. Possible mitigating factors within that decision-making process could be drug use, previous experience with identity theft, or ease of access to the information.

Origin of secondary data

In order to test the hypothesis in this research, analysis was done on secondary data obtained from Interuniversity Consortium for Political and Social Research (ICPSR) and the National Archive of Criminal Justice Data (NACJD). The data was applied for through a “Restricted Use Data Application” from ICPSR, IRB approval was acquired from the UNC-Wilmington IRB board, and data was sent from the NACJD. The original study’s data was collected from 2006 to 2007 on 59 federally convicted identity thieves serving sentences at the time of the study. Copes and Vieraitis conducted the interviews during visits to federal prisons in four different regions of the country utilizing semi-structured interviews. Each offender was
asked the same set of questions the researchers developed, but respondents were allowed lenience on discussion of topics outside of the line of questioning. The typical interview was approximately two hours, although some differentiated due to various factors such as the type of crime the offender was convicted of. The researchers did not compensate the respondents for their participation and IRB protocols were followed throughout the duration of the study. However there were only 49 interviews that were transcribed for the study. Some of the offenders that were originally interviewed by Copes and Vieraitis did not consent to having the interview recorded and others could not be transcribed due to poor recording quality. The original study in which the data were collected for was entitled “Assessing Identity Theft Offenders’ Strategies and Perceptions of Risk in the United States.”

Descriptive characteristics of sample

There were 49 interviews analyzed for this research, including 32 females and 17 males. Of the 32 females, 17 were White, 14 were Black, and 1 was Asian. The male breakdown consisted of 6 White males and 11 Black males. Females almost outnumbered males 2 to 1 in this study, which would fit with the theory that females are more attracted to non-violent crimes as opposed to violent crimes, such as robbery, murder, essentially something with physical harm done to the victim. Within the 49 offenders, 23 were White, 25 were Black, and there was 1 Asian. Racial demographics were reported by the original study’s researchers, Copes and Vieraitis; the respondents did not self-identify these racial categories. Within the sample, 11 respondents self-reported during the interview that they had completed a Bachelors degree or higher, 16 had taken some college courses but not earned a degree, 8 noted they only had a high school diploma, 8 within the sample dropped out of school and never received a high school diploma, and there were 6 respondents who did not indicate their educational background. Most
of the offenders had some type of previous criminal history, although 13 offenders stated this was their first offense and there were no prior arrests. People who used their job in some manner to carry out the theft were not as plentiful as expected, although 20 people out of the 49 cases did use their employment in some fashion to accomplish the crime. Over half the offenders admitted to using drugs during their theft, which consisted of 22 offenders. Prior criminal history was typically limited to drug charges, identity theft charges, property crime charges or fraud charges. There were 4 individuals who had previous drug charges, 5 with identity theft charges, 7 offenders with backgrounds in property crimes, and 13 previously charged with fraud.

Qualitative research

Qualitative research allows the researcher to get a unique perspective from the respondent and allows insight into thoughts and feelings about various subjects. In this particular research dealing with identity theft, we gain perspective on motivations and the respondent’s internal analysis of the crime. That kind of information simply cannot be ascertained from quantitative research as we could only gather responses from Likert-scaled questions rather than being able to notice patterns in thought processes expressed through words.

There has long been a debate over qualitative methods of social research versus quantitative methods of social research. Validity and reliability come into question with each type, yet more people have questions regarding validity and reliability in regards to qualitative data simply due to the nature of analysis. Caroline Stenbecka (2001) addressed these concerns by stating that the overall purpose of quantitative research is a “purpose of explaining,” while qualitative research’s purpose is to “generate understanding” (Stenbecka, 2001:551). Therefore one has to judge each research analysis strategy differently. Some argue that validity and
reliability criteria have no place in qualitative research, rather other factors should be used to judge the quality of qualitative research.

“…while the terms Reliability and Validity are essential criterion for quality in quantitative paradigms, in qualitative paradigms the terms Credibility, Neutrality or Confirmability, Consistency or Dependability and Applicability or Transferability are to be the essential criteria for quality. (Lincoln & Guba, 1985)” (Golafshani, 2003:601)

Like any other debate in academia, the battle between qualitative and quantitative data will likely continue for years to come, although qualitative data is gaining more credibility in the social research field as analysis has become more manageable and user-friendly.

Qualitative data analysis software

The purpose of the analysis was to find common factors amongst identity thieves that could be generalized to the criminal population. These cases were analyzed using MaxQDA to find patterns of commonality and relationships amongst the offenders. MaxQDA is a software package designed to allow users to create their own coding systems for qualitative data analysis. The software operates on the premise of Grounded Theory and qualitative content analysis. MaxQDA was chosen for the analysis of this research due to it being one of the leading programs in advancement of qualitative analysis. Once the data has been coded, it then can be analyzed through various tools to find patterns in the data. The data in this particular research was analyzed primarily looking at motivational factors, such as drug use, prior criminal history, and the ease of the offense.

Analysis strategy

Prior to the data being analyzed by the software, each interview was read in it’s entirety and examined using content analysis. The data was then uploaded into MaxQDA in rich text file format with each interview having an average of 700 paragraphs of text. Each interview was coded using a range of 24 categories such as “prior arrest and criminal history”, “job”, “caught”,

22
“jail”, “method of theft”, “purpose”, “drugs”, “rationalization”, “risk”, “type of ID theft”, and “process”. Those 11 categories were the primary ones utilized in the analysis of the data to find the patterns and themes that were discovered amongst the offenders’ accounts. Using what MaxQDA refers to as “document variables,” that is variables such as demographics that can be linked to each interview document, analysis included demographic information on each respondent such as age, gender, race, drug use, and prior criminal history. Lexical searches were conducted on various strings of text such as “drug use”, “drug habit”, “money”, “bills”, and “support a lifestyle”. Other lexical strings were pieced together to find patterns of motivation, perceptions of risk, ease of the crime, and ideas of punishment for the crime. Once all searches were conducted, patterns emerged from the results, giving way to primary findings for the identity theft research. Further analysis was done on the content of each interview to determine if characteristics of each of the theories presented in this research were present.

RESEARCH FINDINGS

This research aimed to identify factors related to the decision-making process of identity thieves. Upon analysis of the data, certain factors were common to each offender. Every offender interviewed felt the crime was too easy to accomplish and highly addictive. There were rationalization techniques that the offenders utilized to downplay the chances of getting caught. Offenders identified factors within the settings that could be troublesome, such as particular tellers needing to be avoided in banks as well as estimates of how much time a particular transaction should take place. Common factors amongst the thieves were drug usage, prior criminal history limiting risk, lack of understanding of the penalties of the crime, and notions of being too good at completing the crime to get captured. Personal relationships with someone who had access to information or access to information as a result of employment were also key
factors in the decision-making process. Perhaps the most important factor in all offenders’
decision-making process was belief that identity theft is a victimless crime.

After analysis of the interviews, several themes were apparent throughout the data. One strikingly interesting finding was the lack of technological use amongst identity thieves in this study. In the world today technology is a vast part of how people conduct the financial aspects of their lives. Therefore, it is easier than ever to access personally identifying information through the use of computers. Yet, none of these thieves were what would be deemed “hackers”. All individuals interviewed had physical contact with someone to steal the identifying information from the victims. Most of the information came from personal relationships with someone who had legitimate access to the data. However, in some instances there were cases of ordinary street thieves acquiring information to either use themselves or to sell to other criminals. Interestingly the majority of offenders in this study were female. That is not to generalize that identity thieves are more likely to be female, but the characteristic does fit the typical offender committing nonviolent crime.

Methods of access to the information ranged from employee access, such as mortgage officials, Division of Motor Vehicles employees, and bank tellers, all the way to criminals burglarizing a home to gain access to personal records inside the home. Sometimes offenders were posing as representatives of businesses that customers would trust, such as insurance companies and even hospitals. These offenders would pose as an employee to gather information from clients and then utilize the information in their crimes.

Working in groups

Almost all of the offenders in this sample chose to work with a group of people to accomplish their tasks. Very few of them chose to work alone and those that did specifically
cited the risks involved with working with groups as the logic for working on their own. Less than ten percent of the sample worked independently, precisely eight individual cases. The majority of the offenders did indeed work with groups and their logic of group work was there was less risk involved because they could have people going and doing the physical acts of the crime while the offender being interviewed noted they would oversee the people working with them.

Prior criminal history

Ironically there were offenders interviewed that had never committed a crime prior to the identity theft charges. There were only 3 cases of offenders having a prior violent crime charge. Most of those who had criminal history did not have a history of violent offenses. Most offenders noted that they simply could not victimize a person face to face. They felt that the identity theft was a harmless, victimless crime and their rationalization was that the person whose identity they were stealing would be compensated and reimbursed by the bank. The bank would then be reimbursed through their insurance and the only person who would lose out would be the insurance company, which some stated they felt was justified because it was a big business that could afford to lose money.

White-collar crime

Yet the offenders in this sample didn’t always fit the image of white-collar offenders. There were approximately ten percent of the cases in this study that were what would be deemed an ordinary street offender. Over half of interviewees did not earn a college degree and had no special skills one would think a white-collar criminal would possess. However, there were some cases where people would certainly agree that the offender was white-collar. There were
attorneys in the study, mortgage officers, bank loan officers, real estate employees and even a few entrepreneurial investors amongst the offenders interviewed.

Almost all interviewees mentioned feelings of exhaustion near the end of their sprees before being caught by authorities. Some stated that the thefts were a full-time job to them, constantly going to the bank, mailboxes, gathering information, whatever was needed to continue their way of life. Those who were exhausted were actually thankful they got caught because it forced them to quit living the lies they were portraying day in and day out. They admitted that they were unable to stop themselves due to the crime becoming an addiction that was motivating them.

Motivations

The main purpose of this research was to look at motivational factors for the thieves. Several themes became apparent during analysis of motivation for these individuals. The following sections will discuss the breakdown of the motivations, of which one or more were common to most of the offenders in the study. To truly understand how to deter these crimes, we must analyze the reasons behind the offense. Primary motivations were ease of the crime, money, drug use, lifestyle, and supporting family or friends.

Ease of the crime

The vast majority stated the crime was simply so easy they could not stop offending once they began. When questioned about the level of difficulty for accomplishment of the crime imposed on the offender, every single respondent stated that the crime was very easy to pull off without getting caught, or so they initially thought. They were motivated by how simple the task was and how large the payoff became. The notion that purchasing off-the-shelf equipment at local businesses was enough to complete this crime was highly motivational due to ease of
access. Those in the study noted that there was a blatant lack of safeguards to make this task more difficult, as they originally expected it to be.

Money

Obviously one major motivator for the commission of a financial crime is the monetary gain. While this study is not focusing on the broad topic of financial crimes, it is easily evident in society to see the power that money has on humans by examining crimes such as embezzlement and insider trading. Money encourages greed and people take actions they might not take just because money is alluring. There actually was one case in this group of offenders where the thief was utilizing his employment to steal funds and was subsequently charged with embezzlement. However, there was a range of uses within the motivation of money that the offenders were encouraged by. Some needed money to purchase drugs, others needed it to pay bills and some simply wanted to have money around to buy the best of the best of various products on the market.

Money to Support Drug Use
Some were motivated through the habitual use of drugs, mentioning that the drugs allowed them to become numb to the crime and its potential consequences, if those risks were even considered. Those drug addicts also were stealing identities to gain access to money to further their drug use. They simply needed more money quickly and were motivated by the drug desire. Those drug users would then turn around and use the profits from the identity theft to purchase more of their drug of choice. The most common drug usage amongst the interviewees was marijuana and cocaine. Meth was a fairly popular drug of choice as well. While many offenders stated they used drugs, and some in particular were addicted and motivated by drugs, most said the drug was simply a factor in the crime rather than a motivator. Three specific cases mentioned that the drugs were the sole motivator for the crime, while as mentioned
approximately half of the offenders stated they were using drugs during the offenses and it was a supporting factor rather than a primary factor.

Money to Maintain Lifestyle
Others were motivated by the desire to maintain a particular lifestyle, specifically an upper class type of lifestyle. Interviewees working to maintain this lifestyle made mention of expensive cars, large upscale homes, and even brand label clothing. Sometimes these individuals went on exotic vacations and other times they were continuing this façade to maintain their circle of friends they had achieved during this adventure. Twelve out of the forty-nine cases noted they were involved in identity theft to support their lifestyle they were living. Some of these offenders went so far into the lifestyle decision that all the money they had was going to support their image.

“I think at the time I had quite a few homes and quite a few cars and the bills were coming due on everything and I had slacked off for about two months about not getting any money. So I was in a pinch to get the money to pay for the lifestyle I had. I had friends in all of these areas and there was upkeep on stuff. I didn’t want it to all go down, so I took the risk of doing this.” (Respondent 1)

Money to Pay Bills or Help Friends
On occasion throughout the study, a few offenders mentioned they were conducting these thefts to gain access to money to pay bills that were piling up. They felt that they only way they could get out from under their debt was to steal from others. Yet, they mentioned they never felt they were stealing from others. Some of those offenders made note that they intended to pay back the theft by putting money back into the account that they stole from. Several offenders mentioned motivations of helping friends and family; while their motivations may have been genuinely reasonable, their actions resulted in not being able to help their friends and family in the end. Nine of forty-nine offenders were motivated by the need to pay bills and reduce debt or to gain access to money to help friends and family members.
Risks

Commonly amongst the thieves’ views was the notion that there was minimum risk, if they even acknowledged a risk at all. Over three quarters of the interviewees mentioned that they thought they were so good with their actions during the crime sprees that they felt they would never get caught. Some did feel they’d get caught eventually, just not as a result of their own actions. Many mentioned they felt they’d get caught because someone would turn on them and offer information to authorities, which did happen on several occasions. Even those that acknowledged the risks of the crime felt that they would only get a slap on the wrist, mentioning that white-collar sentencing is usually far more lenient. A common misconception among offenders was that they felt they wouldn’t even go to jail but rather they’d get sentenced to house arrest or probation, something that would not require prison time.

“It crossed my mind. See I was on drugs. Yeah. I thought about having to be away from my family, but I ain’t knew it would be this type of impact. I ain’t knew they’d give me this much time. I thought because of a white collar crime, I ain’t think I would get…I thought I’d get a slap on the wrist and like probation or something” (Respondent 2)

In rare cases, some of those offenders interviewed were just conducting their daily jobs and came to find out that they were being charged with a crime because someone in their office, unbeknownst to them, got caught stealing personally identifying information and instead of taking the heat for the crime themselves, that person chose to trade information to investigators for lesser sentencing. Many times in the data, offenders point out that they were not the ringleader of any particular group, yet because a co-defendant implicated him or her, the government took the word of the informant and filed charges accordingly.

Ignorance about the crime

Quite a few offenders indicated remorse for their crime and through the learning process of their extended stay in prison they have come to deal with these feelings and realized that they
should not have victimized people. However there is always the flipside of the coin and the habitual identity theft offenders do exist, some in this study. The government has attempted to combat habitual identity theft offenders though by implementing the crime of aggravated identity theft and structured sentencing for repeat offenders. Aggravated identity theft became a federal crime in 2004 with the addition of statute 18 U.S.C. § 1028A. (Richey, 2010:1) When prosecuted under the aggravated statute, if convicted, there is a mandatory two-year sentencing to be served consecutively to the sentencing for the underlying crime, such as fraud offenses.

Identity theft is a unique crime in itself and many question what identity theft is, including some of the offenders. Under the federal statute 18 U.S.C. § 1028, the United States government prosecutes what it deems identity theft offenders. Yet, through the analysis of this data, the government appears to have a broad range of offenses that can be applicable to this statute. Some were charged with identity theft, when in all practicality they committed credit card fraud. This is a major flaw in the prevention of identity theft, as would-be thieves are not necessarily sure what constitutes a federal offense of identity theft.

Preventative measures taken to minimize risk

Practically every offender in the dataset was actively analyzing the crime, laying out strategies, and planning for the potential to get caught. Some created escape plans to leave the country, some made plans for if they got caught in the banks when cashing checks, and others took precautions to not get caught such as disguises and “throwaway cars” that were purchased for incredibly cheap prices under false names. However there were offenders in the sample that simply did not feel they were at risk of getting caught and therefore those individuals did not take any precautions while performing their crimes.

A complete definition of all subsections of 18 U.S.C. § 1028A is provided in Appendix B.
Those that utilized their employment to complete the theft took precautions such as working only with people they trusted in other companies, such as a real estate agent hand choosing the lawyer, mortgage officer and appraiser in order to have less risk of getting caught.

On occasion those that went into the banks would choose specific characteristics that they would look for in a bank teller, such as age, race, and gender. They felt they had better chances of success with specific qualities and characteristics in a person. This type of thought process is indicative of rational choice theory. These offenders were actively analyzing the cost and benefits of each stage of their crimes. Rationally figuring out that disguises and “throwaway cars” would help to diminish the possibility of getting caught shows forethought by the offender as to how to successfully accomplish their end goal.

“Throwaway accounts, that’s what I’d call them. I also had throwaway cars. I would buy little two, three hundred dollars cars that had those people’s license plates still on them and then I would go through drive-thrus so if they tried to track me, it was just a car I would just take and park around the block or just leave it and just dispose of it. And so I would take and purchase them in cash, you know two or three hundred dollars and not give the person my information as to who they sold it to. I would give them somebody else’s information and so I would just take. I had throwaway phone too. Those prepaid throwaway phones that can never be traced…” (Respondent 3)

Rational choice theory

Overall, the offenders did follow a rational thought process guiding their decision-making. They developed plans to accomplish goals, gathered important data, recruited additional personnel to assist, and even had escape plans in place. They appeared to rationally decide that the risks were not enough of a deterrent in comparison to the personal gains they would make from the identities stolen. As previously mentioned in the rational choice theory discussion, part of the decision making process for the offender is which category they would like to be placed in. According to Cornish and Clarke (1985), they must either be criminally involved or a criminal
actor. Some of the offender noted that they were involved in the identity theft, but didn’t actually carry out the theft of the information. Yet, the government charged them with conspiracy to commit identity theft, which still carries prison sentencing. Those that were charged by the government, as conspirators, argued that they were not involved nor were they an actor in the crime. The interviewees rationalized their actions to themselves at the time by assuring themselves that it is not their job to inform the government of someone’s wrongdoings. However, apparently the government will not show lenience towards criminally involved conspirators in the battle against identity theft.

Bounded Rationality

Offenders in this research sample could certainly be viewed as rational in their decision-making, but that rationality was bounded by their perceptions and knowledge at the time of the decision. They simply could not have known every possible factor at the time of making choices, such as when the offenders mentioned they would leave the bank during a check fraud if the teller asked too many questions or if the teller approached the bank manager. Their bounded rationality told them that they were going to get caught, but yet they had no idea of actually knowing what was being discussed between the teller and the manager, unless they overheard the conversation. Other times bounded rationality existed when offenders were out searching mailboxes looking for identity information in various neighborhoods. They had no way of knowing who would be around at any given time, but they acted upon their choice that they felt they would not get caught based upon picking particular times of day, such as when people should have been at work.

Self-control theory and impulsivity

Self-control theory appears to not be applicable to the overall group of offenders in this particular sample of identity thieves. It is worth noting that there were a few cases that
mentioned they were addicted to the crime and could not stop until they were arrested. This would show a lack of self-control amongst these specific individuals. However, impulsivity was not present amongst any of the offenders’ recounts of their crimes. These criminals were the exact opposite of impulsive; they were methodical and careful about their crime, yet not careful enough as they got caught. Self-control was analyzed using content analysis looking for characteristics described by the theory.

**Employment**

While employment at a job that would grant access to identities of others was hypothesized to be a major factor in the beginning of this research, findings showed that offenders did use employment as a means to carry out the theft, but not the theft of identifying information. Some of the offenders in the sample who had access to information as result of their job noted that they did not gather any information from their place of employment because they felt it would have victimized their bosses and they didn’t feel that was ethically correct. In cases such as these, offenders who did not want to victimize their bosses sought out conspirators who had access to information through other means and conducted the offense outside of their job.

However, just because they did not gather personal information on victims from their job did not rule out the use of their employment to carry out the identity theft. Approximately 40 percent of respondents in the research stated that their employment contributed to the identity theft. Most of these cases were offenders who worked in real estate or mortgage type situations. These offenders were typically convicted of mortgage fraud, appraisal fraud, and in some cases identity theft.
DISCUSSION

Identity theft is a crime that has gained the interest of thieves and the general public over the last two decades. Yet, it’s only been within the last few years that credit monitoring services have appeared and have gained popularity with the masses. Although, that does not mean that everyone has some type of this service, nor does it mean that people realize just how endangered their information truly is. Some people navigate through life rarely checking their credit until they intend to use it, but by that point if something has gone awry it is very difficult to get fixed, especially if time is of the essence. The government has made some headway by imposing stricter laws and tougher sentencing, but only time will tell as to how effective they are in combating this particular crime.

Offender discussion

It was blatantly apparent in the analysis that someone can complete this crime without a formal higher education using nothing but street knowledge. The offenders were reasonably rational in their thought processes from start to finish, however they were not careful enough as they got captured. It perhaps is comforting to understand that identity theft is not something that one will go out and commit on an impulse. They may carry out pieces of the crime on impulse, such as going and stealing someone’s mail out of a mailbox, but the vast majority of the crime must be thought out and meticulously planned. Yet, their rationale for the acts was varied among a few categories as previously mentioned. Some wanted money solely for the purpose of going out and spending it on drugs. They could have been the lowest person in the operation, getting the least profit from the crime, but they still did it to earn money for their drug of choice. Others fixated on the materialistic symbolism that they wanted to exude. Those offenders had to have the nicest, newest things on the block no matter the cost. Those offenders that were focused on
physical items could be classified as offenders committing crimes to support a lifestyle, as previously referred to in this research. Lifestyle offenders use their financial gains to further their personal habits, which could be drugs, alcohol, houses, cars, or anything of the sort. Obviously there are incredibly different lifestyles each offender could lead, however all lifestyle motivations stem from the desire to ignore social norms such as responsibility.

CONCLUSIONS

Identity theft is a dangerous crime threatening the safety and security of one’s financial means and lives. If someone falls victim to identity theft, they could end up in such a position in life that they cannot even afford to feed and clothe themselves and their loved ones. Social Security numbers, which are issued to each and every person in the United States, were not created with the intent to be utilized in such a manner as they are in current times. They are used everywhere on plenty of documents and citizens think nothing of filling out a form for various businesses with their Social Security number on it. Employment applications, educational applications, loans, insurance; these are just a few of the things that people encounter dozens of times in their lives that request such sensitive information.

Differences from Copes and Vieraitis (2007)

This research differed from Copes and Vieraitis (2007) by focusing solely on the qualitative method of the analysis and attempting to gain an understanding and insight into the motivations that drive the offender to make the choices they do to commit identity theft. The expectation originally was that self-control theory would be far more applicable than it ended up being. While self-control theory did not pan out as was hoped, there was still some slight evidence of impulsivity, a key component of self-control theory. Copes and Vieritis (2007) had
the intent of analyzing the offender’s notions of the risks involved, while this research was
driven by analysis of motivational factors.

Recommendations

A goal of this research was to offer recommendations to limit the potential prevalence of
this crime in the future. Throughout the findings, there were several themes that showed areas
where improvements could be made, both in research and in policy. These themes have been
analyzed to determine the implications they have in their respective fields and recommendations
to remedy these implications have been established. There is simply not enough research being
done on the crime of identity theft to fully understand every aspect that needs to be explored. In
order to limit the prevalence of this crime, we have to reduce the opportunities presented to these
thieves. Newman and McNally (2005) note that to reduce opportunities society must increase
situational prevention. Society must make the offender work harder to achieve the completion of
the crime, increase the likelihood of capture, reduce the reward that the offender gains from the
crime, reduce temptations luring offenders and finally remove the rationalizations offenders
utilize for justification of their criminal act, (Newman and McNally, 2005:80). Due to the
evolving nature of society, identity theft is going to be a continuous game of one-upmanship for
years to come.

Future Research Implications

As Copes and Vieraitis (2007) were conducting interviews, the federal government
created a new provision in the fight against identity theft. The crime of “aggravated identity
theft” was created which carried a mandatory minimum sentencing of two years. Future research
is needed to determine whether or not this addition is limiting the prevalence of identity theft. It
is not truly known how many cases of identity theft take place each year because it is an under
reported crime, but also because these identity thieves are not captured as often as the general
public would like them to be. Research cannot solely rely on incarceration rates of the offenders that are arrested for identity theft and its various subcategories.

Research could also be conducted to determine how the corporate and banking environments are reacting to the threat of identity theft and what preventative measures have been examined, or even put into place, to stop thieves before they ever gain access to valuable information. Unfortunately large amounts of this type of information are unlikely to be available due to the nature of confidentiality of the security measures. However, there are most likely some preventative steps that have been taken that could be researched for effectiveness to limiting access to personally identifying information.

Future Policy Implications
Identity theft is a highly evolved crime with the days of electronic banking, computer technology, and ease of access to information. Throughout this research, many different holes have been discovered in the system that ordinary people do not even think are there. Criminals know these weaknesses and exploit them to better their own situations. Banks should increase security on their computer systems and networks, as you constantly hear of banks having security breaches and having to issue new account numbers to clients. Perhaps there is a way to add multiple layers of security to accounts that are being accessed by clients, both on the Internet and at local branches. A possibility is adding passwords on the accounts before money could be removed. This would only feasibly work if there were a way to require facial recognition and the password, perhaps through the use of video calling technology. This is certainly a farfetched idea, but it could indeed be a new wave of the future of security. Department stores and big box stores must figure out a way to secure in-store credit applications, as many of the thieves that were interviewed for this research noted that it was incredibly easy to obtain a credit card
account for any particular store they frequented. Most did not request identification, and a computer station set up in the business processed the applications immediately.

Identification
On the topic of identifications, state-issued driver’s licenses and identification cards must be safeguarded to the point where duplication is impossible to the average criminal. There were interviewees that stated they printed identification from their personal computer, and some even went to print shops and had duplicates made. While technology can be an enemy and threat to our security, it can also lend a helping hand to defend against intrusions of our personal information. One could only imagine what identification will be like in the next twenty years. The advances in years past have worked to an extent, yet they can still be replicated. Those advances that were thought to be game-changing were holograms on identifications, barcodes, and even watermarks. Yet, in the interviews, prisoners noted they were able to duplicate some of these fail-safes to the point that it was undetectable that the identification they were using was a fake. Some of those duplicates that were made at the print shops were “cleaned” through the use of chemical solutions to make them appear as though they were state issued. Simply put, not enough is being done to prevent false identification production. Other inmates reported they had people connected inside the Division of Motor Vehicles to print identifications for their use. While it is impossible to prevent people from being corrupt, you could punish those corrupt individuals so severely that the other people in the industry realize that the risk is not worth the gain. This is just one possible way to increase deterrence.

Financial Institution Security
Banks apparently are a severe problem when it comes to identity theft. Citizens all around the world leave their money with banking institutions with the trust that they will safeguard one’s life earnings, yet banks are not doing everything in their power to keep those
accounts secure. Checking accounts are becoming more electronic and less paper intensive. Checks are becoming a thing of the past with the advent of direct deposits, debit cards, and electronic transfers. Yet, checks are still accepted at banks and many retail outlets worldwide. A simple piece of paper with numbers printed on the bottom just out in the open with no safeguards. The financial industry must figure out a way to secure checks, whether it is to change the acceptance policies or simply abolish them all together. Quite a few of the interviewees were convicted of check forgery, noting that all they needed to know was an account number, a routing number, and the name on the account and they could duplicate a check. There is software readily available designed to create checks for businesses and this software can be purchased both at retail locations and online with shipping straight to one’s doorstep. Blank checks can be obtained for an average citizen to print their own checks. A couple of the interviews mentioned that the defendants were editing already printed checks that they stole out of the trash or mailboxes. They would “wash the check”, essentially removing the ink from certain parts and rewriting their own information into it and using it as a newly written check. The financial industry is not the only player in this game that should be blamed, but they are a major part of it.

Enforcement
The government has to increase their punishments for identity theft, but also they must go after the physical leaders of these organizations. Many of the interviews had statements from the convicted individuals mentioning that they were accused of being a ringleader of a particular group, but they were not. While it is possible for one to simply say they were not the leader and didn’t have full knowledge as a way of rationalizing their actions to themselves, most offered compelling arguments as to why they were not the head of the organizations or groups. It appears as though the government does want to prosecute people for identity theft, but they
simply want someone to place the blame on rather than spending the time to prosecute the appropriate members of society who are purporting this horrendous crime that sticks with a victim for years. There also was no consistency with sentencing of these identity thieves. Some major players were given lesser sentencing simply because they turned on their codefendants faster than the rest. That does not send the message of deterrence; rather it sends the message that it is acceptable to commit this crime as long as you confess to it first, so you can secure your decrease in sentencing compared to the rest of those involved.

Furthermore, identity theft itself must be more concisely defined. Many different crimes were being prosecuted under the branch of identity theft. Anything from conspiracy to commit fraud to forgery to actual identity theft, where one is assuming the identity of another and living under stolen information, has been prosecuted under the Identity Theft Assumption and Deterrence Act of 1998. While giving a more concrete definition will not necessarily do anything for prevention, it at least informs the general public about the actions that will constitute penalties for identity theft. Quite a few of the prisoners mentioned they were unaware they would get as harsh of sentencing as they did, as they were under the impression that white collar crimes simply got a slap on the wrist and possible probation.

Educating the Public

Once a concise definition of identity theft is created, the government can then begin to educate the general public about the crime as well as its repercussions. A public service announcement or educational program should be created to inform the masses about the severity of this crime. Never before has access to personal information been so easy and the criminals know that. In order to prevent the majority of offenders from acting upon the urge, the government must educate them on the penalties associated with breaking identity theft laws. The general public must also be knowledgeable about how to protect their personal information from
falling into the wrong hands. While nothing is foolproof, citizens the world over must realize how preciously valuable their identifying information is and the potential frustrations they could endure should they not heed the warnings to safeguard that information.

Using employment to further crime
Both legal statutes and corporate policies should be put into place to punish those who utilize their employment to further their criminal venture. While there are some laws that could be used against employees who steal things from their job and use their position of power to commit crimes, a specific case against those who foster identity theft should be made. As a society, identity theft must not be tolerated, especially from people who are supposed to be trusted with identifying information that could damage one’s financial well-being. A provision could even be built into the federal statutes making one’s employment a factor for sentencing, with harsher penalties being handed down to those who used their employment to benefit their crime.
References


Cornish, Derek, Ronald Clarke. 1985. Rational choice theory. Chapter 1. 10


Stanford University Press.


Appendix A

Identity Theft Assumption and Deterrence Act of 1998

18 USC § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information

(a) Whoever, in a circumstance described in subsection (c) of this section—

(1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;

(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;

(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;

(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;

(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification;

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under subsection (a) of this section is—

(1) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is—
(A) the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be—

(i) an identification document or authentication feature issued by or under the authority of the United States; or

(ii) a birth certificate, or a driver’s license or personal identification card;

(B) the production or transfer of more than five identification documents, authentication features, or false identification documents;

(C) an offense under paragraph (5) of such subsection; or

(D) an offense under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period;

(2) except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 5 years, or both, if the offense is—

(A) any other production, transfer, or use of a means of identification, an identification document, authentication feature, or a false identification document; or

(B) an offense under paragraph (3) or (7) of such subsection;

(3) a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed—

(A) to facilitate a drug trafficking crime (as defined in section 929 (a)(2));

(B) in connection with a crime of violence (as defined in section 924 (c)(3)); or

(C) after a prior conviction under this section becomes final;

(4) a fine under this title or imprisonment for not more than 30 years, or both, if the offense is committed to facilitate an act of domestic terrorism (as defined under section 2331 (5) of this title) or an act of international terrorism (as defined in section 2331 (1) of this title);

(5) in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and

(6) a fine under this title or imprisonment for not more than one year, or both, in any other case.

(c) The circumstance referred to in subsection (a) of this section is that—

(1) the identification document, authentication feature, or false identification document is or appears to be issued by or under the authority of the United States or a sponsoring entity of an event designated as a special event of national significance or the document-making implement is designed or suited for making such an identification document, authentication feature, or false identification document;
(2) the offense is an offense under subsection (a)(4) of this section; or

(3) either—

(A) the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or

(B) the means of identification, identification document, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.

(d) In this section and section 1028A—

(1) the term “authentication feature” means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;

(2) the term “document-making implement” means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;

(3) the term “identification document” means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;

(4) the term “false identification document” means a document of a type intended or commonly accepted for the purposes of identification of individuals that—

(A) is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and

(B) appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;

(5) the term “false authentication feature” means an authentication feature that—

(A) is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit;

(B) is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document,
document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or

(C) appears to be genuine, but is not;

(6) the term “issuing authority”—

(A) means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and

(B) includes the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization;

(7) the term “means of identification” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A) name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e));

(8) the term “personal identification card” means an identification document issued by a State or local government solely for the purpose of identification;

(9) the term “produce” includes alter, authenticate, or assemble;

(10) the term “transfer” includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others;

(11) the term “State” includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States; and

(12) the term “traffic” means—

(A) to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value; or

(B) to make or obtain control of with intent to so transport, transfer, or otherwise dispose of.
(e) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title.

(f) Attempt and Conspiracy.— Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

(g) Forfeiture Procedures.— The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(h) Forfeiture; Disposition.— In the circumstance in which any person is convicted of a violation of subsection (a), the court shall order, in addition to the penalty prescribed, the forfeiture and destruction or other disposition of all illicit authentication features, identification documents, document-making implements, or means of identification.

(i) Rule of Construction.— For purpose of subsection (a)(7), a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification.
Appendix B
Aggravated Identity Theft Statute

18 USC § 1028A - Aggravated identity theft

(a) Offenses.—

(1) In general.— Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2) Terrorism offense.— Whoever, during and in relation to any felony violation enumerated in section 2332b (g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

(b) Consecutive Sentence.— Notwithstanding any other provision of law—

(1) a court shall not place on probation any person convicted of a violation of this section;

(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used;

(3) in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised in accordance with any applicable guidelines and policy statements issued by the Sentencing Commission pursuant to section 994 of title 28.

(c) Definition.— For purposes of this section, the term “felony violation enumerated in subsection (c)” means any offense that is a felony violation of—

(1) section 641 (relating to theft of public money, property, or rewards [1]), section 656 (relating to theft, embezzlement, or misapplication by bank officer or employee), or section 664 (relating to theft from employee benefit plans);

(2) section 911 (relating to false personation of citizenship);

(3) section 922 (a)(6) (relating to false statements in connection with the acquisition of a firearm);
(4) any provision contained in this chapter (relating to fraud and false statements), other than this section or section 1028 (a)(7);

(5) any provision contained in chapter 63 (relating to mail, bank, and wire fraud);

(6) any provision contained in chapter 69 (relating to nationality and citizenship);

(7) any provision contained in chapter 75 (relating to passports and visas);

(8) section 523 of the Gramm-Leach-Bliley Act (15 U.S.C. 6823) (relating to obtaining customer information by false pretenses);

(9) section 243 or 266 of the Immigration and Nationality Act (8 U.S.C. 1253 and 1306) (relating to willfully failing to leave the United States after deportation and creating a counterfeit alien registration card);

(10) any provision contained in chapter 8 of title II of the Immigration and Nationality Act (8 U.S.C. 1321 et seq.) (relating to various immigration offenses); or

(11) section 208, 811, 1107(b), 1128B(a), or 1632 of the Social Security Act (42 U.S.C. 408, 1011, 1307 (b), 1320a–7b (a), and 1383a) (relating to false statements relating to programs under the Act).