GEOGRAPHIES OF IDENTITY THEFT IN THE U.S.:

UNDERSTANDING SPATIAL AND DEMOGRAPHIC PATTERNS, 2002-2006

A Thesis

by

GINA W. LANE

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

December 2008

Major Subject: Geography

GEOGRAPHIES OF IDENTITY THEFT IN THE U.S.:

UNDERSTANDING SPATIAL AND DEMOGRAPHIC PATTERNS, 2002-2006

A Thesis

by

GINA W. LANE

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Approved by:

Chair of Committee,	Daniel Sui
Committee Members,	Robert Bednarz
	Jim Olson
Head of Department,	Doug Sherman

December 2008

Major Subject: Geography

ABSTRACT

Geographies of Identity Theft in the U.S.:

Understanding Spatial and Demographic Patterns, 2002-2006. (December 2008)

Gina W. Lane, B.S., Texas A&M University

Chair of Advisory Committee: Dr. Daniel Sui

Criminal justice researchers and crime geographers have long recognized the importance of understanding where crimes happen as well as to whom and by whom. Although past research often focused on violent crimes, calls for research into non-lethal white-collar crimes emerged in the 1970s. Today, identity theft is among the fastest growing white-collar crimes in the United States, although official recognition of it as a criminal act is a relatively recent development. Remaining largely unmet, the need for white-collar crime research has greatly intensified considering the escalating identity theft problem. Furthermore, many studies conclude that identity theft will continue to rise due to increasing technology-driven offenses via the Internet and widespread use of digital consumer databases. Utilizing theoretical framework established in crime geography, GIS mapping and spatial statistics are employed to produce a spatial analysis of identity theft in the U.S. from 2002-2006.

Distinct regional variations, such as high rates in the western and southwestern states, and low rates in New England and the central plains states, are identified for identity theft as reported by the FTC. Significant spatial patterns of identity theft victims

alongside social demographic variables are also revealed in order to better understand the regional patterns that may indicate underlying social indicators contributing to identity theft. Potential social variables, such as race/ethnicity and urban-rural populations, are shown to have similar patterns that may be directly associated with U.S. identity theft victims.

To date, no in-depth geographic studies exist on the geographic patterns of identity theft, although numerous existing studies attempt basic spatial pattern recognition and propose the need for better spatial interpretation. This thesis is the first empirical study on the geographies of identity theft. It fills in a void in the literature by revealing significant geographical patterns of identity theft in the digital age, attempts at understanding the social factors driving the patterns, and examines some of the social implications of identity theft.

DEDICATION

To my daughters, Noelle and Michelle, for all that we have endured together,

my parents, Wilmer and Lovelle Walterscheid, for their unconditional love and support throughout the years,

Sarah Bednarz, for truly inspiring me towards higher education,

and for my beloved husband, Mitch, who, in his sacrifice to our nation, enabled me to pursue this degree

ACKNOWLEDGEMENTS

I want to kindly thank my committee chair, Dr. Daniel Sui, to whom I especially express gratitude for welcoming me as his student and offering exceptional guidance and advice throughout. It has been a true honor to work with him. I also thank my committee members, Dr. Robert Bednarz, and Prof. Jim Olson, for their guidance, instruction, support, patience, and belief in my abilities throughout this research. I could not have succeeded without all of you. Your teachings brought me to where I am today.

Many thanks, also, to all of my friends and faculty at Texas A&M, who have welcomed and supported me throughout the years. Thank you, to everyone who offered support, advice, and friendship as a fellow student and friend. In particular, I graciously thank Nikki Williams and Adriana Martinez for their enduring friendship, support, and encouragement over the years. People like you make anything possible.

NOMENCLATURE

ESDA	Exploratory spatial data analysis
FTC	Federal Trade Commission
GIS	Geographic information system
IDW	Inverse distance weighting
LISA	Local indicators of spatial association
MAUP	Modifiable areal unit problem
MSA	Metropolitan statistical area
VIF	Variance inflation factor

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

> It is every type of crime but with a component placing it in the digital environment. It is able to operate instantaneously, remotely, and with disregard for sovereignty and geography.
>
> (Len Hynds 2003, pg. 4)

Identity theft disrupts the lives of thousands of people each year. Unfortunately, no one, either alive or deceased, is immune from the threat (O'Brien 2004, DPS 2008). Overall, identity theft has become one of the fastest growing crimes in the United States, and has been the top consumer complaint in the U.S. since the year 2000 (Computer Fraud & Security 2008; Welborn 2004). Furthermore, when considering the known links between identity theft, terrorism, and homeland security, the potential victims of identity theft may indirectly extend towards the entire U.S. population.

Despite the seemingly ubiquitous prevalence of identity theft in the digital age, distinct regional patterns exist, which this study further examines (Mulrean 2006). Historically, many crime studies rely on crime mapping and a social ecology approach towards explaining the local physical and social conditions at high crime hotspots. Generally speaking, place-based crime theories seek to identify the local conditions that facilitate the confluence of victims and offenders in time and space (Anselin et al 2000). Interestingly, regional variations and hotspots for identity theft also persist, even though identity theft is unique in that victim-offender relationships can be, and often are, geographically decoupled. This is possible because unlike traditional theft, identity

---

This thesis follows the style of *The Professional Geographer.*

thieves often surreptitiously employ hi-tech technologies such as computers and the Internet to inflict damage on unsuspecting individuals. Although not all identity theft incidences occur via cyberspace, significant amounts do. Therefore, alongside many other changes brought about by onset of the digital age, cyber crimes, such as identity theft conducted over the Internet, have the potential to break down traditional spatial barriers for crime, such as locational opportunity and victim-offender proximity. This phenomenon is indicative of crimes conducted over the Internet, as traditional theft crimes are spatially dependent. Overall, cyber crimes (although not limited to identity theft) have the ability to transcend physical spatial limitations potentially creating virtually limitless and anonymous links between victims and offenders. Theoretically, cyberspace could eliminate the importance of place for crimes such as identity theft, yet the persistence of clear regional patterns indicates that place (e.g. local populations) remains important.

Regardless of the growing prevalence of identity theft, official recognition of it as a criminal act is a relatively recent development, and academic researchers have been slow to respond to the growing threat. In 1998, the federal government passed the Identity Theft and Assumption Deterrence Act (H.R.4151 and S.512, henceforth referred to as The Identity Theft Act), which officially defined and established identity theft as a criminal act punishable by law. The Identity Theft Act also established the Federal Trade Commission (FTC) as the lead agency to monitor, track, analyze complaints, and disseminate information to consumers, researchers, and law enforcement agencies

(United States 105th Congress 1998). Since 2001, the FTC has logged increasing identity theft complaints, publishing the figures in annual clearinghouse reports (Table 1). By the year 2006, over 1 million complaints had been cumulatively logged (Conkey 2006).

Table 1: Federal Trade Commission Annual Identity Theft Complaints

Year	Total Complaints	Annual Change	Percent Change
2002	161,896	--	--
2003	215,093	53,197	+32.85%
2004	246,570	31,477	+14.63%
2005	255,565	8,995	+3.65%
2006	246,035	-9,530	-3.73%

Although scholarly publications regarding identity theft are limited, much of the literature that exists comes from governmental studies, criminological research, or popular media (Cheney 2003; FTC 2003; Mulrean 2006; Newman & McNally 2005; Synovate 2003). To date, no known spatial identity theft studies have been published in any geographic journals, although publications from other disciplines and in the popular media often exhibit geographic observations, attempt some degree of spatial interpretation, or propose the need for better spatial analysis. For example, Mulrean (2006) states that identity theft is typically more urban than rural, has regionally high per-capita levels in the southwestern United States and low per-capita levels in the Central Plains, and may be affected by age. Newman and McNally (2005) observe that identity theft rates vary internationally, and call for additional research into the geographic and demographic trends that are outlined by the FTC and Synovate Reports (2003). Allison et al (2005) call for additional research to determine whether the demographic findings in their study are localized or nationally representative. This thesis, therefore, fits well into the literature as a response to these calls for taking a more explicitly geographic perspective on identity theft research. This information is vital in formulating generalizations that may aid in determining effective strategies to address the growing identity theft problem at broader levels.

This thesis fills a void in the literature by advancing our understanding of significant geographical patterns of identity theft in the digital age. The specific goals of this research are:

1) Identify unique spatial and temporal patterns of identity theft in the U.S.;
2) Explore the social and demographic factors that may shape the regional patterns of identity theft in the U.S.;
3) Discuss the social implications of identity theft and its relationship towards terrorism and homeland security.

This thesis explores the geographic frontiers unique to identity theft, and will also establish identity theft spatial inquiry within geographic crime and identity theft literature. Furthermore, the findings of this study will provide a basis from which further analysis into the social factors of identity theft can be explored, and facilitate effective policies of fighting and preventing this prevalent white-collar crime in the digital age.

2. BACKGROUND AND LITERATURE REVIEW

2.1. Defining identity theft

What exactly is identity theft? Many have attempted to address this essential question, and as a result, there are numerous attempts at defining what is (and is not) identity theft. Researchers generally agree that identity theft involves the fraudulent misuse of personal information for illegal activity and unauthorized personal gain, but some debate exists on where to 'draw the line' on what constitutes identity theft. For example, Cheney (2003) argues that the simple use of a person's bank or credit card account for unauthorized transactions should not be considered identity theft, but rather should be considered the simpler crime of payment fraud. In another more unconventional interpretation of the problem, Caeton (2007) presents the bold argument that identity theft is not the victim-offender phenomenon popularized in the media. Rather, he posits that identity theft is actually a cultural myth, created by the politics of fear, in which the long-standing white-collar crime of fraud has been bureaucratically re-codified as victim-offender 'identity theft' in order to shift the blame away from a lack of systematic safeguarding of personal data, which would solve the so-called identity theft problem. Although extreme, Caeton does exemplify the wide range of defining views regarding the position of identity theft as a stand-alone crime.

For the purpose of this research, however, the crime of identity theft is assumed to be real and prosecutable (Hynds, 2003), and the definitions established by federal law will be used to ensure consistent and proper analysis of the FTC data. According to the Identity Theft Act:

> [Identity theft occurs when someone] knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law (United States 105th Congress 1998, p. 2-3).

Table 2 lists the officially recognized FTC categories and sub-categories. The FTC data makes no distinction within the categories or sub-categories regarding the severity of the incidences or type of personal information that was used. Additionally, the sum of category complaint percentages may exceed 100% (thus also exceeding the number of actual victim complaints) due to some reports logging multiple categories of damages per incidence; however, each victim is only counted once per complaint, regardless of how many categories that were involved, thus providing an accurate overall victim complaint count. It is within this framework of the Identity Theft Act definition and the subsequent development of the categorized FTC database, that I conduct this research (Table 2).

Table 2: FTC Categories and Sub-Categories of Identity Theft

Major Category	**Percent of Total* (value) 2002**	**Percent of Total* (value) 2006**	**Sub-Categories**
Credit Card Identity Theft	42% (68,100)	25% (61,509)	– New accounts, existing accounts, unspecified
Phone or Utilities Fraud	22% (35,617)	16% (36,365)	- New wireless, New telephone, Unauthorized charges to existing accounts, Unspecified
Bank Fraud (checking, savings, EFT)	17% (27,522)	16% (36,365)	- Existing accounts, Electronic Funds Transfer (EFT), New accounts, Unspecified
Employment-Related	9% (14,571)	14% (34,445)	- No sub-categories
Government Documents or Benefits Fraud	8% (12,952)	10% (24,604)	- Fraudulent tax return, Driver's license issued/ forged, Government benefits applied/ received, Other government documents issued, Social Security card issued/ forged, Unspecified
Loan Fraud	6% (9,712)	5% (12,301)	- Business/ Personal/ Student loan, Auto loan, Real estate loan, Unspecified
Other Identity Theft	16% (25,903)	24% (59,048)	- Illegal/ Criminal, Internet/ e-mail, Medical, Apartment/ house rented, Insurance, Property rental fraud, Bankruptcy, Child support, Magazines, Securities/ investments

Source: Federal Trade Commission (http://www.ftc.gov/bcp/edu/microsites/idtheft/)
*Percentage sums exceed 100 due to individuals reporting multiple victimizations

2.2. Crime geography and criminology literature

Criminologists and geographers alike have long realized that understanding where crime happens is key to understanding why crime happens and to whom (Christens & Speer 2005; Roncek 1993). Therefore, criminal justice researchers and geographers have understood the analytical and predictive roles of crime mapping (Anselin et. al 2000; Harries 1974, 1999; Lottier 1938a, 1938b; Shannon 1954). In general, geographic crime studies and crime mapping seek to accomplish three main goals: description, analysis, and prediction (Harries 1974). The main goal of descriptive mapping is to identify patterns, trends, and facts from the data. Initial assessment of the data via GIS mapping and analytical methods, often called exploratory spatial data analysis (ESDA), is the first step in geographic crime study, and is the main goal of this research. Second, analytical mapping accomplishes the goal of hypothesis testing in order to develop a base from which predictions are made. It is the theoretical bridge between description and prediction mapping. A secondary goal of this research is to establish enough geographic links between identity theft and demographic patterns to allow for future hypothesis formulation for further study in order to accomplish the ultimate goal of prediction, which is likely the most valuable product from a successful geographic crime study or model (Harries 1974).

Historically, crime geography theory has passed through several major periods. The earliest studies, mainly conducted in the 19^{th} century, were mostly environmentally deterministic (Anselin 2000; Cohen 1941; Harries 1974). Geographers attempted to explain observable seasonal and regional crime patterns through variations in the physical environment, such as climate, topography, or latitude. Critics soon emerged, and after the turn of the 20^{th} century, the era of environmental determinists waned. In its place emerged the social theorists, largely originating from the Chicago School.

Early social theorists incorporated the role of human conditions, such as urban environments, distance decay, and population characteristics, to explain local crime patterns (Cohen 1941). In general, social human phenomena were used to provide an ecological explanation of crime patterns by linking existent local conditions to observable spatial patterns (Harries 1974; Cohen 1941). Later, detailed regional studies emerged which not only incorporated social conditions, but particularly emphasized regional spatial patterns of crime at multiple scales (Lottier 1938a, 1938b; Shannon 1954). Eventually, more radical geographic studies incorporated complex social science theories, such as the impact of social control systems, into geographic crime patterns (Lowman 1986). However, some debate exists on the effectiveness of applying social theory in crime study. Critics posit that it offers little new insight into violent crimes (Harries 1986) and does not explain differential responses (Herbert 1982). For example, if social factors such as race, income, or family structure, are determined to cause criminal behavior, why are not all people with these characteristics criminals? According to Herbert (1982), this is a major shortcoming of using social theory in geographic crime studies.

Regardless, a renewed interest in spatial crime study based on social theory is currently underway. Anselin et al (2000) largely attributes the renewal to recent analytical and technological improvements. Better computing capabilities, powerful geographic information systems (GIS), and specialized spatial tools enable researchers to analyze large databases that were previously unmanageable, and reemphasize the importance of place-based crime studies. As a result, Anselin et al (2000) states that geographic crime study is "… currently in the midst of a Chicago School revival…Though not causally related, recent developments of widely accessible computerized mapping and spatial analysis techniques have accompanied the resurgence in popularity of ecological explanations of crime" (p. 218). This thesis, therefore, will contribute towards this emerging body of renewed spatial crime analysis.

Throughout the evolving theoretical eras, most geographic crime research has focused on violent crimes (Christens and Speer 2005; Harries 1988; Snook et al 2005), with an emphasis on determining either treatment or causation (Herbert 1982). Treatment research is usually an empirical criminology approach whereby mitigation strategies or actions are applied and analyzed for effectiveness through observed changes in the targeted criminal activity. Causation research, however, is much more ambiguous, and attempts to identify characteristics and causes of criminal activity from data collected from known offenders, victims, and criminal behavior patterns. Herbert (1982) definitively states that researchers should keep offender and offense pattern analysis separate, and that analysis of offenses (e.g. victims) is particularly suited for geographic study (pp. 44, 101). This is because offense patterns lend themselves largely to local conditions facilitating vulnerable environments, opportunities for crime, access routes, and criminal methods, thus allowing for spatial insight towards broader societal problems that facilitate the formation of vulnerable populations. In other words, knowing where a certain crime is occurring is clue to discovering underlying social indicators facilitating the criminal behavior.

Despite that violent crime studies have dominated past research, calls for better spatial research into non-lethal white-collar crimes emerged as early as the 1970s (Peet 1975; Herbert 1982). Remaining largely unmet since then, the need for white-collar crime research has greatly intensified considering the escalating identity theft problem

(FTC 2007). The FTC data indicates that identity theft overall is steadily increasing; however, critics argue that increased public awareness is attributable to the rise in reporting frequency due to improved legislation, consumer education, and improved law enforcement reporting practices (Stana 2004). Although this may partially explain the longitudinal increase in reports, Allison et al (2005) acknowledged this possibility and found substantial evidence that "… suggested an increasing trend for identity theft cases relative to other types of theft offenses" (p. 24). Furthermore, many studies conclude that identity theft will likely continue to rise due to increasing technology-driven offenses via the Internet and illegal data mining of digital databases containing consumers' personal information (Cheney 2003; Liu, et al 2005; Norum and Weagley 2007; Slosarik 2002). Clearly, the need for research into the geographic trends and underlying driving mechanisms of identity theft are overdue.

2.3. Identity theft and white-collar crime literature

2.3.1. Identity theft literature

Identity theft is "[t]he quintessential crime of the information age…" (Kahn and Roberds 2008, p. 251). Increasing use of electronic transactions, over the Internet and through the direct use of credit and debit cards, generates millions of opportunities every day and has vastly increased the risk for breach and misuse of personal information by identity thieves (Anderson 2006). As a result, consumer reports of identity theft have increased dramatically, bringing much attention to the problem by the media, government agencies, and general public. Until Slosarik (2002) published an overview, thus establishing identity theft as topic for academic research, scholarly publications specific to identity theft were virtually non-existent. Since then, a growing body of identity theft literature has emerged, which includes (but is not limited to) offender and victim trends and demography (Allison et al 2005; Anderson 2006), systemic enabling factors and solutions (Bourne & Deaton 2004; LoPucki 2002; Willox and Regan 2002), preventative and protection efforts (Milne 2003; Milne et al 2004; Norum and Weagley 2007), financial system and consumer impacts (Cheney 2003), regional and behavioral patterns (Mulrean 2006), computer modelling (Kahn and Roberds 2008), and legislative efforts (Holt 2004; Moye 2006; Saunders & Zucker 1999). This thesis will contribute the first known empirically geographic study of identity theft to the growing body of identity theft literature.

Although many agree that the recent widespread growth of identity theft has been largely "E-enabled" (Pemble 2008, p. 7) by the advance of the digital age, identity theft itself is not new (Pemble 2008; Caslon Analytics 2008; Caeton 2007; Friedrichs 2007). History is riddled with accounts of identity imposters whereby individuals fraudulently assumed the literal identity of another for personal gain. What has changed, however, are the available methods used to commit the offense. Technological advances such as the Internet and computers have drastically increased the ease and efficiency by which offenders illegally obtain personal information (Slosarik 2002; Norum and Weagley 2006; Pemble 2006). Identity thieves digitally reach beyond political boundaries, bypassing security measures in place to thwart illegal movements of people, information, and goods. These technological abilities contribute to the increase in identity theft, and are the enabling mechanisms for the decoupling of victims and offenders. No longer is it necessary for an individual to literally assume the living identity of, or be in contact with, another person in order to benefit from the assumption of personal information.

A person's identity involves social and personal associations such as nationality, ethnicity, gender, race, age, and socioeconomic status. Identity is also a legal issue. Legal identity is delineated by official documents, paperwork, activity files, etc. and is essentially unalterable. Legal identity takes precedence over social identity in the courts and is virtually inescapable, such as a criminal record or credit history. It is the targeting of the legal identity, increasingly becoming digitally obtainable, which enables identity theft activity (Finch 2003).

Identity theft involves the fraudulent use of base identifiers: birth name, race, birth date, etc. Base identifiers remain unchanged over an individual's lifetime. Secondary identifiers, such as drivers' licenses, passports, visas, and green cards rely on base identifiers to connect to the individual. As the population has increased, base identifiers have become insufficient in uniquely identifying all individuals. Therefore, numerical identifiers were introduced as a means to uniquely classify individuals in large populations. In the U.S., the social security number (SSN) is the most important and ubiquitous numerical identifier. Although the initial intent of the SSN was not as a universal identifier, the current amount of personal information associated with it makes it the "linchpin in advancing identity theft" (May and Headley 2004, p. 13). Since all legal citizens in the U.S. have these numerical identifiers, yet identity theft does not appear to target victims randomly, a better understanding of the characteristics those experiencing higher rates is needed.

In general, offenders are known to utilize a wide array of techniques to illegally obtain personal information about their victims. Traditional, low-technology methods continue to persist and include mail fraud, ‘dumpster diving’ (retrieving discarded documents), stolen wallets/purses, and obtaining information through personal contacts (known as social engineering) (Javelin Strategy & Research 2006). High-technology methods using computers and the Internet (e.g. scams, malicious spyware, and illegal ‘data mining’ of digital databases, etc), have greatly expanded the ability for identity thieves to remotely access personal information (Allison et al 2005; Cheney 2003; Furnell 2007; Slosarik 2002), and are widely believed as the vehicles enabling the recent explosion of identity theft. In sum, the Internet has increased the speed, ease, and efficiency of identity theft. As the opportunity for high-technology offenses is expected to increase, the more tedious, low-technology methods are likely to become less appealing.

Although identity theft is largely motivated by pecuniary want, the damages victims experience are both financial and non-monetary, such as false arrests, social denunciation, collection agency harassment, credit denials, and loan refusals (Kreuter 2003; Newman & McNally 2005; Slosarik 2002), not to mention time lost correcting the damage, and personal distress (Furnell 2007). Like many crimes, actual measurement of the extent of identity theft is difficult due to suspected low rates of reporting and the tendency for identity theft incidents to be multi-faceted, which may result in multiple reports per victim (FTC 2003; Hayward 2004; Newman & McNally 2005; Stana 2004). Besides financial motivation, there are other known motivating factors. Some identity thieves have been known to desire a 'fresh start' from an undesirable past. Others are seeking alternative identities in order to clandestinely engage in illegal activity (Finch 2003). This last motivating factor is particularly important in understanding the role which identity theft plays in terrorism, a topic that will be discussed at length below (Sullivan 2004; Collins 2006; Willox & Regan 2002).

Better understanding of identity theft is critical in order to thwart the continued growth of the crime. Identity theft is expected to increase into the unforeseeable future largely because of a plethora of existing electronic databases that contain vital personal information. Many of these databases do not have adequate security for protection against either internal or external data thieves. International and inter-jurisdictional outsourcing of jobs also potentially increases the security threat (O'Brien 2004), and the tendency for identity theft to occur inter-jurisdictionally and in conjunction with other crimes often prevents the ability for lawmakers to specifically target it. The resulting low prosecution and clearance rates, coupled with lenient sentencing, have created an environment conducive to rampant identity theft (Collins 2006). In 2000, only one in 700 identity theft crimes were prosecuted, meaning that the potential rewards are very high while the risk remains incredibly low (Sullivan 2004). Since clearance rates are not rising at the same rate that reports of identity theft are, this figure is expected to worsen.

It is obvious that identity theft is a very real and rapidly expanding problem in the digital age. The broad range of disciplines producing studies and publications is indicative of its pervasive nature and broad extent, and clearly points toward the benefits of additional spatial and demographic inquiry.

2.3.2. Demographic observations in white-collar crime literature

The identification of demographic associations are commonplace in many white-collar crime studies in general, and identity theft studies in particular (Acohido 2007; Allison et al 2004; Anderson 2006; Ganzini et al 2001; Newman and McNally 2005; Synovate 2003; Weicher 2007; Willox and Regan 2002). Demographic variables of both victims and offenders exist in the literature, although it is unknown whether victim and offender patterns are related. Therefore, demographic subsets suggested in the literature for both victims and offenders are utilized in building the demographic database for this study, as known offender characteristics may indicate linked victim population subsets.

Because the majority of identity theft incidences are considered white-collar crimes, a review of white-collar crime literature is important and offers helpful insight towards a better understanding of identity theft in particular. The term 'white-collar crime,' first coined by Edwin Sutherland (1940), was initially defined by the social class of the criminals themselves. Challenging dominant philosophy, Sutherland proposed that criminal activity is not caused by poverty or the social woes of the lower classes, but exists among members of all social strata, including the middle and upper classes. Sutherland proposed a distinction between "…crime in the upper or white-collar class, composed of respectable or at least respected business and professional men, and crime in the lower class, composed of persons of low socioeconomic status" (1940, p. 1), and introduced the concept of non-violent, largely financial offenses to scholarly social and criminological research.

Since Sutherland's introductory research, a concise definition of white-collar crime has proven elusive, but modern definitions focus not only on the social class of the offender, but also on the nature of the crime itself. Generally, white-collar crimes occur within a legitimate occupational environment, are economically motivated, and do not involve physical violence (Friedrich 2007). The majority of identity theft offenses certainly meet these criteria. Therefore, identity theft is considered a white-collar crime, although not all white-collar crimes involve identity theft.

Unfortunately, research into white-collar offender demographics has been hindered by a lack of comprehensive data. Low prosecution and conviction rates, coupled with low reporting rates of white-collar crimes by both victims and law enforcement, have resulted in a virtual dearth of comprehensive data (Croall 2001). The available data is largely based on known offenders and consumer reports, may be affected by prosecution, judicial, and law enforcement biases, and is consequently not randomly generated. For example, Green (1993) suggests that offender clearance rates for embezzlement may be affected by demographic factors of age, gender, and race.

Regardless of data shortcomings, researchers have revealed some demographic trends for white-collar criminals. Known characteristics of white-collar criminals differ from conventional 'street' and violent criminals. White-collar criminals are usually older, rarely have prior arrests, and are often highly educated. White-collar criminals are often members of higher socioeconomic groups, thus introducing social stratification associations (Friedrichs 2007). Although offenders are less likely to be drug addicts than street criminals, researchers recognize that drug addiction may increase the likelihood of financially motivated crimes and identity theft (Croall 2001; NDIC 2007; Payne 2003).

Although a significant number of offenders are male members of 'elite' social classes, they do not comprise the entirety. Many are middle class females and are often employed in lower-level clerical positions. For example, bank embezzlers tend to be younger, female, and living in stable home environments (Croall 2001). Although the criminal male typecast persists, in reality more women commit fraud than men, and researchers have found that women are more likely than men to be motivated by personal reasons such as financial need (Croall 2001).

White-collar criminals also have different age and racial profiles than conventional criminals (Croall 2001, Friedrich 2007). White-collar criminals are usually older with racial profiles similar to the general population. White offenders tend to be from higher socioeconomic groups, while black offenders are more often from lower socioeconomic groups. Most attribute the socioeconomic differences largely to employment discrimination. Regarding the age of offenders, one U.S. study revealed the average age of all white-collar offenders to be forty years; however, mail fraud and embezzlement offenders tended to be younger (Croall 2001). It is possible then, that identity thieves may be slightly younger than other white-collar criminals.

Despite the fact that many white-collar offenses go unreported, victim data is more comprehensive than offender data. From existing data, researchers have discovered that different white-collar crimes are known to target specific groups. For example, women have historically been victimized by financial fraud due to presumed assumptions that women are not as knowledgeable about finance and investing as are men. Additionally, older cohorts have been targeted by financial fraud, largely because older citizens often have higher incomes and greater wealth, thus making them attractive targets (Croall 2001, p. 74). There is some concern that victim reporting may be biased towards higher educated individuals due to the fact that they are more likely to possess the knowledge and resources to report and prosecute the offense. Regardless, white-collar crime victims appear to be a population subset with identifiable demographic characteristics, which provides the basis for the creation of the demographic database for this thesis.

2.3.3. Demographic observations in identity theft literature

Identity theft is not an equal opportunity crime. Although the FTC clearinghouse reports reveal some associations between identity theft complaints and demographic trends, this thesis seeks to further investigate demographic links to identity theft. The literature suggests an abundance of demographic observations warranting further examination. For example, general trends in identity theft are known such as urban propensity, exceptionally low clearance rates, and localized demographic characteristics such as gender, age, and race (Allison et al 2005). Social indices such as level of urbanization, socio-economic status, and family structure have been identified as potentially related factors for criminal behavior in general (Glaeser and Sacerdote 1999).

Studies have shown that some age groups are higher risk for identity theft (Table 3):[1]

[1] These figures are approximate and may vary slightly depending on the data year. Other researchers have revealed similar figures for different years, e.g. May and Headley 2004.

Table 3: Frequency of Identity Theft within Age Cohorts

Age Group	Percent of Victims	Percent of Total Pop	Representation
0-17	2 %	26.4	Under
18-29	26 %	15.8	Over
30-39	28 %	15.4%	Over
40-49	22 %	15.1%	Over
50-59	13%	11%	Over
60+	9%	16.3%	Under

Sources: Stana 2004; U.S. Census Bureau, decennial census data 2000

College students have also been targets of identity theft because of widespread institutional use of social security numbers, plus students with clean credit records are often targeted by credit companies, and young students may be relatively naïve regarding financial decision-making (Weicher 2007). Certain occupations have also been found to carry a higher risk for identity theft. High-paying professions such as physicians and celebrities have been targeted, as well as professions that offer personal information more easily such as university professors and government employees (May and Headley 2004). Case studies of particular incidents illustrate this well. For example, Abraham Abdallah, 32, stole the identities of over 200 celebrities listed in the "Forbes 400," eventually accessing potential billions of dollars before being caught in 2001. In 2002, Linus Baptiste, 43, co-conspired with Philip Cummings, 32, to steal the identities of 33,000 victims by obtaining user names and passwords through employment at a credit-checking communications company. In 1998, Anthony Lamar Taylor, 30, successfully posed as golf superstar Tiger Woods for a year before getting caught (Sullivan 2004).

Some studies specifically examine the demographics associated with identity theft (Table 4). Allison et al (2005) examined the demographic trends of both victim and offenders in a particular Florida metropolitan area with intriguing results:

Table 4: The Demography of Identity Theft in a Florida Metropolitan Area

Demographic Variable	Victims	Offenders
White	72%	27%
Black	20%	69%
Hispanic	1%	1%
Asian	6%	1%
Female	46%	63%
Male	54%	37%
Mean Ages	40.56	32.23

The Hispanic population was especially recognized as underrepresented because 19-percent of the metro area population is Hispanic, yet there was a negligible Hispanic representation (only 1-percent of both victims and offenders) in the identity theft data. Whites were overrepresented as victims (72-percent), and blacks were overrepresented as offenders (69-percent) in this study. Lastly, the study also revealed that 53-percent of the offenders were unemployed, 3-percent retired, and another 3-percent were disabled. This suggests economic gain as a motivator for identity theft. (Allison et al 2005).

Anderson (2006) suggests that demographic variables (e.g. income and education level) are viable proxies to test for populations vulnerable to identity theft, such as the hypothesis that people who conduct more non-cash transactions and utilize numerous accounts are more at risk for identity theft. Anderson also suggests that single heads of households and households with children may also be more vulnerable. This is based on the idea that couples have double the eyes and attention to discover identity theft, and children create additional transactions, each of which, although minute, poses a new opportunity for a breach of personal information. Using probit regression, Anderson concluded that families with three or more children had a significantly higher risk for identity theft. Other social groups suggested in the literature as potential high-risk groups for identity theft include people living in close group quarters such as students (Newman and McNally 2005; Norum and Weagley 2007; Weicher 2007) and military members, (Acohido 2007; Newman and McNally 2005), medical patients (Ingram 2006), and even the deceased (CIFAS 2004; DPS 2008; O'Brien 2004).

In sum, victims of identity theft are members of a population subset which may be partly determined by certain underlying geographic and/or demographic characteristics. By identifying which demographic characteristics may be disproportionately associated with identity theft, researchers may be able to predetermine those most at risk. This may lead to potentially revealing more complex associations and insight beyond that of statistical and exploratory data analysis (EDA).

3. DATA AND METHODOLOGY

3.1. Data

This research is conducted with data from two primary sources:

1) Identity theft data from the FTC
2) Demographic data from the U.S. Census Bureau

The Federal Trade Commission releases annual identity theft clearinghouse reports (available from: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/index.html). The majority of complaints are logged via direct consumer input to the FTC, however other organizations also contribute, including the U.S. Postal Inspection Service, Internet Crime Complaint Center (www.ic3.gov), plus others (FTC 2004, 2005). Preliminary examination of the data revealed visible regional variations, thus prompting the need for an in-depth spatial analysis to determine whether the visible patterns can be significantly explained through exploratory spatial data analysis (ESDA) and statistical analysis.

Demographic data was mostly obtained from the U.S. Census bureau website. The census data was acquired directly from the American Factfinder (factfinder.census.gov), and population estimates (www.census.gov/popest/estimates). Whenever possible, the demographic data was obtained for the corresponding year of FTC data; however, when estimates are not available, Census 2000 data was used.

The FTC identity theft data are aggregate, and the FTC clearinghouse releases identity theft figures at national, state, and MSA scaled levels. Because this study analyzes the state-level identity theft data, the demographic data was amassed at the corresponding state-level scale.

3.1.1 Data issues and challenges

Because the data is aggregate, it is imperative to acknowledge potentially related problems. Certain challenges and concerns are endemic to aggregate data, and can be particularly troublesome for spatial analysis. First, aggregate data is secondary, meaning that it has undergone some processing of the raw data beforehand (Rafanelli et al 1996). The algorithms used in the pre-processing of the data is often unknown (i.e. the data sets are released without metadata), and it is possible that the methods used to create spatial aggregations (such as statewide counts, sums, averages, categorizations, etc), may affect the final aggregate values.

In regards to the spatial analysis of aggregate data, perhaps the greatest concerns stem from the Modifiable Areal Unit Problem (MAUP) (Openshaw & Taylor 1982). The MAUP exists because geographic space can be divided into potentially infinite arbitrary units. Since geographical space is continuous, the analysis of data collected within that space can be greatly affected by the scales and/or zones of the data aggregation (Openshaw & Taylor 1982), which can potentially be manipulated by the analyst in order to produce favorable outcomes (Anselin 2006). Data aggregated by political units, such as the statewide FTC data, is confined to a priori boundaries, which cannot be manipulated by the analyst, but it is unlikely that these boundaries will have any direct relationship to the spatial phenomenon being observed.

For example, a spatial study conducted by a private industry fraud detection service, ID Analytics (2007a), illustrates the effects of the MAUP well. Using credit application data and fraud detection models, ID Analytics determined rates of application fraud, thus producing a geography of offenders rather than victims. When analyzing the fraud rates at the statewide level, the results were very similar to the FTC victim patterns. States with high rates of fraudulent applications included the western states of WA, OR, CA, NV, AZ and TX, plus NY, IL, and MI. States with very low rates of fraudulent applications included the upper New England states of ME, NH, VT and the northern plains states of ID, MT, WY, SD, and IA. However, when analyzing the same raw data at smaller scales, (the 3- and 5-digit zip code levels) the results were quite different. As the scale becomes smaller, strong regional patterns became much less prevalent, to the point where at the smallest scale 5-digit zip code level, contradictory findings emerged. At the 5-digit zip code level, high fraudulent application rates originated from states that were considered overwhelmingly low overall. In fact, the zip code with the second highest fraud risk in the U.S. from 2003-2006 was in South Dakota, a state which is considered consistently low in identity theft risk. A second ID Analytics (2007b) report identifies the top ten 5-digit zip codes with the highest identity fraud increases in 2006. Six were in Montana, and three were in North Dakota, (also recognized in other studies as low-risk states), again showing that small-scale analysis of the same data can yield very different results than coarse scale. It is unknown if similar spatial trends could be found with the FTC identity theft data, as the FTC does not release it at selectable scales such as the Census Bureau.

Understanding the MAUP leads into another problem inherent to aggregate data: the ecological fallacy. The ecological fallacy problem states that "…conclusions obtained at aggregate levels do not translate to meaningful behavioral interpretations at the micro scale" (Anselin 2006, p. 4). Researchers have long recognized problems in assuming characteristics of the individual from aggregated data of larger populations, and for this reason, the findings from this thesis cannot be used to infer information about small populations or individuals.

Certain problems inherently exist with most crime databases as well (Harries 1974; Herbert 1982). For example, recall that under-reporting and misreporting (by individuals, victims, or authorities) are concerns for the data being under-representative of the true extent of identity theft. Also, differences in attitudes and classification methods across jurisdictions and/or agencies could affect the data, and could also impart spatial irregularities if these classification differences vary regionally. There also exists concern that changes in reporting practices, public awareness, and legislation could affect data collection, particularly data that is amassed temporally as in the FTC Consumer Sentinel. Despite these challenges, official aggregated data, such as the FTC clearinghouse, is the only known data source publicly available, leaving no viable alternatives.

Regardless of the limitations of aggregate data, the FTC data is considered the most comprehensive identity theft data in existence (Newman & McNally 2005). To date no known comprehensive database of identity theft incidences with demographic data exists; therefore, aggregate data must be utilized, largely due to a dearth of nonaggregated data and the difficulty or impossibility in obtaining such data. Regardless, the significant correlations revealed by this study between demographic groups and known identity theft incidences may provide opportunities for additional research or case studies to explore more specific associations.

3.1.2 Identity theft data

As per the requirements of the Identity Theft Act (United States 105th Congress 1998), the FTC established the Identity Theft Clearinghouse, and in 1999 began to amass consumer complaints into a large centralized database called Consumer Sentinel (FTC 2003). The majority of complaints are logged via direct consumer contacts with the FTC, however numerous other agencies also contribute (FTC 2003, 2004, 2005). The FTC then categorizes the data by different types and subtypes, separating identity theft related fraud from other types of fraud, and annually releasing the figures to the public via clearinghouse reports, which are available from the www.ftc.gov identity theft reference desk.

It is important to note that data included in the FTC identity theft categories and sub-categories, such as credit card, phone utilities, and bank fraud are amassed separately from fraud incidences that do not involve the misuse of personal information. For example, Consumer Sentinel logged in excess of 635,000 complaints in 2004, 39-percent of which were fraud by identity theft, with the remaining 61-percent being non-identity theft fraud complaints. In sum, not all fraud complaints involve the misuse of personal information, and are not included in the identity theft database; however, the FTC uses the term “fraud” interchangeably within the identity theft and non-identity theft data, thus potentially causing some confusion in the category definitions.

Although the FTC data is the most complete central repository of identity theft data currently in existence, it is still believed to be under-representative of the true scope of identity theft incidences, and may have some reporting errors due to multiple-agency contributions (for example, if a consumer contacts multiple agencies, thus generating multiple counts per incident) (Newman &McNally 2005). Despite that the FTC data does not represent the actual scope of the identity theft problem[2], researchers conclude that it is substantial for spatial analysis and the identification of geographic trends (Allison et al. 2003). To date, truly representative data are lacking due to a combination of hurdles. A lack of coordinated interagency cooperation exists, and white-collar crimes (identity theft in particular), are beset by low reporting and clearance rates, thus hindering capture of all incidences and posing difficulties in the creation of unbiased, comprehensive datasets (Allison et al 2005; Newman & McNally 2005; Slosarik 2002).

The aggregated identity theft database for this project was created by harvesting the annual figures from the FTC clearinghouse reports. Unfortunately, the report formats are not consistent, thus requiring some data extraction for 2002, 2005, and 2006. For these years, individual state data were released as linked state maps, whereby the data was obtained by manually selecting each state individually from the online base map.

[2] Realizing that the scope of identity theft is likely much higher than the complaints logged by the Consumer Sentinel, the FTC commissioned Synovate, (a global market research firm under Aegis Group) to conduct a nationwide poll to determine a more accurate extent of identity theft. From this study, annual incidences of identity theft in the U.S. are estimated at over 9 million (Synovate 2003).

From 2002 through 2004, the state data and identity theft categories were reported as actual victim counts. However, for 2005 and 2006, the data was released as state victim totals with category percentages. Therefore, the derivations of actual victim counts by category for each state were calculated by multiplying the identity theft category percentages by the total victim counts. For example, in 2005, Arizona logged 9,320 victims, with 26-percent reporting credit card theft, or 2423.2 victims for the credit card category. Since the existence of a fraction of a victim is not feasible, the derived counts are rounded up to the next integer, thus introducing the existence of a small rounding error for the 2005 and 2006 data. Cumulatively, the rounding error is slight and is unlikely to affect the analysis results.

The final database encompasses annual FTC identity theft data from 2002 through 2006, reported as state-level figures broken down by FTC category (Table 2).

3.1.3 Demographic data

The demographic variables (or proxies) suggested in the identity theft literature acted as guidelines for the selection of potential demographic variables for this study (Appendix 2) from which an extensive database was built using data obtained from the U.S. Census Bureau and Progressive Policy Institute (PPI) (www.ppionline.org). The majority of demographic data for this study was obtained through the U.S. Census Bureau (http://www.census.gov/). Whenever possible, Census population estimates for the demographic variables are obtained to better correlate with the identity theft reporting years. However, the Census Bureau does not produce estimates for all population subsets, in which case Census 2000 data was utilized. The Digital Economy

Index scores (DigEcon) and online population (OnlinPop) were obtained from the Progressive Policy Institute (PPI), a governmental non-profit research and education organization that produces a State New Economy Index as a means of calculating U.S. states' progression towards a digital economy (PPI online). The Digital Economy variables were obtained based on the literature which states that the Internet is a key element in the rise in identity theft.

3.2 Methodology

This study fits well and addresses research gaps within the literature of both crime geography and identity theft research. Overall, by utilizing theoretical framework established for crime geography (Harries 1974, 1999), addressing the calls for better spatial analysis of identity theft (Newman and McNally 2005; Allison et al 2005), and expanding research knowledge of existing identity theft/demographic studies (Allison et. al 2005; Anderson 2006), this project seeks to contribute a social ecology spatial analysis to the nascent body of identity theft research. The goal is to identify significant spatial patterns of identity theft victims alongside social demographic variables in order to determine correlated spatial patterns that may reveal underlying social indicators contributing to this pervasive crime. By using spatial statistics techniques and GIS mapping, distinct regional variations are identified for identity theft as a whole, as well as for the FTC classification categories. Additionally, statistically significant correlations reveal potential social variables, such as race/ethnicity and urban-rural population composition, that may be directly associated with identity theft victims in the U.S. from 2002 through 2006.

3.2.1 Selection of significant demographic variables

The purpose of this phase of the analysis is to determine correlations between the demographic data and the identity theft data. To accomplish this, traditional statistical tests were performed using the master database (containing both demographic and identity theft data) to determine which variables return significant correlations (see Appendix 2 for complete list of results). Using identity theft per capita rates (by category and by year) as the dependents (y), and demographic variables as the independents (x), SPSS software was employed to run both uni- and multi-variate regression analyses in order to narrow down the demographic variables to a more specific quantity. The null hypothesis being tested was that the slope of the regression line is zero (H_o: $\beta_1 = 0$), thus indicating no correlation if the p-value is greater than $\alpha = .05$ for a 95-percent confidence level. For the years 2002 and 2006, by holding the per capita identity theft dependent variable constant and repeatedly running regression analyses for each demographic variable, a concise list of correlated variables were identified for overall identity theft per capita rates and also for each of the subcategories. These tests were repeated for both years in order to determine if the patterns are static or are temporally evolving.

The use of per capita rates in lieu of actual incident counts has been common practice throughout crime mapping research (ID Analytics 2007a, 2007b; Lottier 1938a, 1938b; Shannon 1954). The method retains validity because per capita figures are normalized by current population counts, thus representing the rate of identity theft by an intensity ratio within each state for a specific year, regardless of state population differences. For example, one would expect more occurrences of a phenomenon in a highly populated state such as California, than in a state with a low population, such as Vermont. By comparing ratios, a better representation is achieved which accounts for population differences. Therefore, per capita rates are a good indicator of the pervasiveness of the crime within each state.

Linear regression is chosen as the appropriate and optimal statistical tool since all variables involved are continuous (e.g. categories such as race, urban/rural are measured as either actual population counts, or on a 100-scale percentage such as per-capita values). The variables were further tested for residual normality, constant variance, collinearity, extreme outliers, and extreme leverage values. The result was a concise, workable demographic database (Table 5) with all variables showing significance in relation to the identity theft data with particular attention paid to potential problematic issues, such as heteroscedascity or collinearity in the data.

Table 5: Demographic Variables Correlated with Identity Theft Categories

Variable	**Definition**	**Highest Correlation R^2 Value with Per Capita Identity Theft Rates**
CredIssu	Number of businesses issuing credit	.458
DigEcon	Digital Economy Index score	.344
HISP_pct	Percent of population that is Hispanic	.782
HspEst	Hispanic Population Estimate	.434
HspFamSz	Average statewide family size, head of household Hispanic	.333
MilBarak	Population living in military group quarters	.311
OnlinePop	Online population	.400
UrbanPct	Percent of population living in urban areas	.622

3.2.2 GIS mapping

GIS mapping was conducted in order to visualize regional patterns in the data. ArcGIS 9.0 was used to create the maps by joining the master database containing both identity theft and demographic data to appropriate shape files for each mapping technique. For the identity theft data, a set of maps was produced for both 2002 and 2006 data. A set of maps was also produced for the selected demographic variables.

Choropleth maps were first created for both identity theft and demographic data by joining the master database to a polygon shape file of the 48 contiguous U.S. states. Alaska and Hawaii were omitted from the mapping as they are geographically detached from the mainland and therefore cannot be part of a regional cluster. The choropleth maps were produced using six classes (quintiles method), or eight states per classification. The use of equal count classification quintiles is a commonly used method for regional crime mapping, dating as far back as Lottier (1938a, 1938b). The quintiles method is chosen here to reveal regional patterns as the classes are not based on an arbitrary value (which would vary by year), but are selected solely on the basis of state membership for each class based on the data for that year. The initial maps revealed that regional differences are most prominent for identity theft data when normalized with population values (producing per capita equivalent values).

Understanding, however, that information flows and identity theft patterns likely do not adhere to political boundaries, a secondary set of spatially interpreted maps is needed in order to reveal regional patterns independent of arbitrary state borders. Inverse distance weighting (IDW) is chosen as the spatial interpolation method here. IDW is based on Tobler's First Law of geography, which posits that things closer together in space are more related than things farther away (Tobler 1970). In IDW, values at known locations are used to interpolate expected values at points in-between. Values nearer to the point to be interpolated will have more influence than points farther away, and the weighted influence of points (or neighbors) is determined by the value of the weighting parameter. Specifically, IDW is defined as:

$$z' = \frac{\sum_{i=1}^{N} z_i * \frac{1}{d_i^r}}{\sum_{i=1}^{N} \frac{1}{d_i^r}}$$

Where d = distance between given and observed points; z = observation point; N = number of observations; i = iteration; z' = weighted value at the given point; and r = weighting parameter.

Unlike choropleth mapping which requires polygon data, spatial interpolation requires point data. To create the point file, state population centroids were extrapolated based on the populations of the top identity theft reporting cities in each state (according to the FTC). The master database was then joined to the state centroids shape file, thus providing for spatial interpolation via inverse distance weighting (IDW). The resulting maps are continuous raster surfaces showing regional patterns of identity theft intensities across states. As with the choropleth maps, six classes were designated using the quintiles method in order to maintain comparability of the mapping techniques. Because the IDW method is unable to interpolate beyond the outermost point, the centroids in Washington, California, Maine, and Florida were manually nudged to prohibit mid-state truncation of the interpolation raster surface. The resulting maps reveal distinct regional variations in the data similar to the comparable choropleth maps.

3.2.3 Spatial statistics analysis

The third level of analysis for this research employs spatially specific procedures in order to detect significant clustering and/or outliers within the data. This procedure is necessary to corroborate the findings of the GIS maps, and to further analyze the data with specialized spatial statistical tools in order to mathematically bolster the patterns and clusters identified with ArcGIS. LISA analysis is excellent for identifying hot spots, geographic clusters, and spatial outliers (Anselin 1995), which is particularly apropos to the patterns observed in the ArcGIS analysis.

GeoDa, a spatial statistics package developed by the Spatial Analysis Lab at the University of Illinois, was utilized to apply local indicators of spatial autocorrelation (LISA) to the data. LISA analysis specifically examines the spatial aspects of data by linking individual observations to global measures via spatial weighting matrices, and works well in both spatial pattern exploration and confirmation (Anselin 1995). LISA is often used to analyze the spatial characteristics of large spatially referenced data sets. However, Anselin (1995) shows that it is also effective in the analysis of smaller datasets ($n < 50$), by using LISA to successfully reveal spatial patterns of conflict amongst 42 African countries. Therefore, LISA is an appropriate tool for this project where $n = 48$, composed of state polygons. The LISA results corroborate the findings of the GIS mapping and the initial regression analyses to ensure that the regional patterns and clusters revealed in the GIS mapping are true and mathematically supported, and not merely a product of cartographic manipulation.

LISA analysis can be executed on either original data, as in this thesis, or standardizations. LISA incorporates neighborhood analysis and distance weighting in the calculations whereby the tests are specifically designed to determine significant regional clustering and/or outliers within the data.

Specifically, in GeoDa univariate LISA is defined as:

$$I_i = \frac{(x_i - \mu_x)\sum w_{ij}(x_j - \mu_x)}{\sum_j (x_j - \mu_x)^2 / n}$$

where x are observations, and w_{ij} is a spatial weights matrix equal to $1/d_{ij}$ in which d_{ij} represents the Cartesian distances between the ith and jth points. The spatial weights matrix for a polygon shape file can be either Rook (common boundary) or Queen (common boundaries and vertices), or can be based on the distance between points, such as polygon centroids (Figure 1).

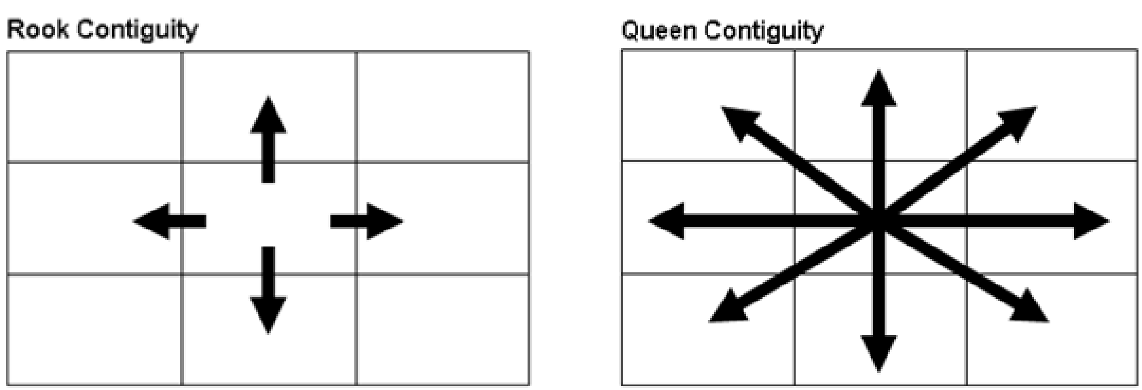

Figure 1: Rook vs. Queen Contiguity

For this thesis, all three spatial weights methods were explored. Queen continuity produced the best results, capturing more accurate state neighborhoods because all states do not share common boundaries, yet are considered neighbors at one or more vertices (e.g. UT, AZ, CO, and NM).

In the results, a positive I_i value indicates a spatial clustering of similar values (similar high or similar low values), while a negative I_i value indicates a spatial clustering of dissimilar values, such as when a high value is surrounded by neighbors with low values, or vise versa. Thus, the LISA I_i value reveals clusters of either stability (similarities) or outliers of instability (dissimilarities) in the spatial data.

4. RESULTS AND DISCUSSIONS

4.1. Results

Overall, regional patterns were clearly identified. Consistent with the earlier media reports, the desert southwest states appear to maintain the highest per capita rates, while the plains states and upper New England have the lowest per capita rates. Some of the subcategories show unique patterns. For example, there was an eastern shift in identity theft in the form of government document fraud by 2006, which analysts believe is a result of a sharp increase in fraudulent government benefit claims after Hurricane Katrina (Conkey 2006). The highest demographic correlations were with states with higher Hispanic populations.

4.1.1. Identifying unique spatial and temporal patterns

The ArcGIS maps revealed existing regional patterns in the identity theft and demographic data. On the whole, identity theft patterns appear to be relatively static from 2002 through 2006, however, some categories do exhibit spatial changes.

When looking at actual identity theft counts, no clear regional patterns emerge. Rather, states with the highest populations, such as California, Texas, Florida, New York, Illinois, and New Jersey consistently and expectedly report high numbers of identity theft complaints. However, by normalizing the identity theft complaints by the population, a common long-term practice in past regional studies, per capita rates of identity theft are produced, which offer a better representation of the varying statewide intensities of the crime (ID Analytics 2007a; 2007b; Lottier 1938b). These maps revealed that the per capita rates of identity theft do exhibit clear regional variations (Figure 2). The normalized data reveal two distinct regional patterns of identity theft. The desert southwest and western states exhibit much higher rates, and the middle and northern plains and upper New England states typically report much lower rates for both 2002 and 2006.

Actual Identity Theft Counts | Per Capita Rates

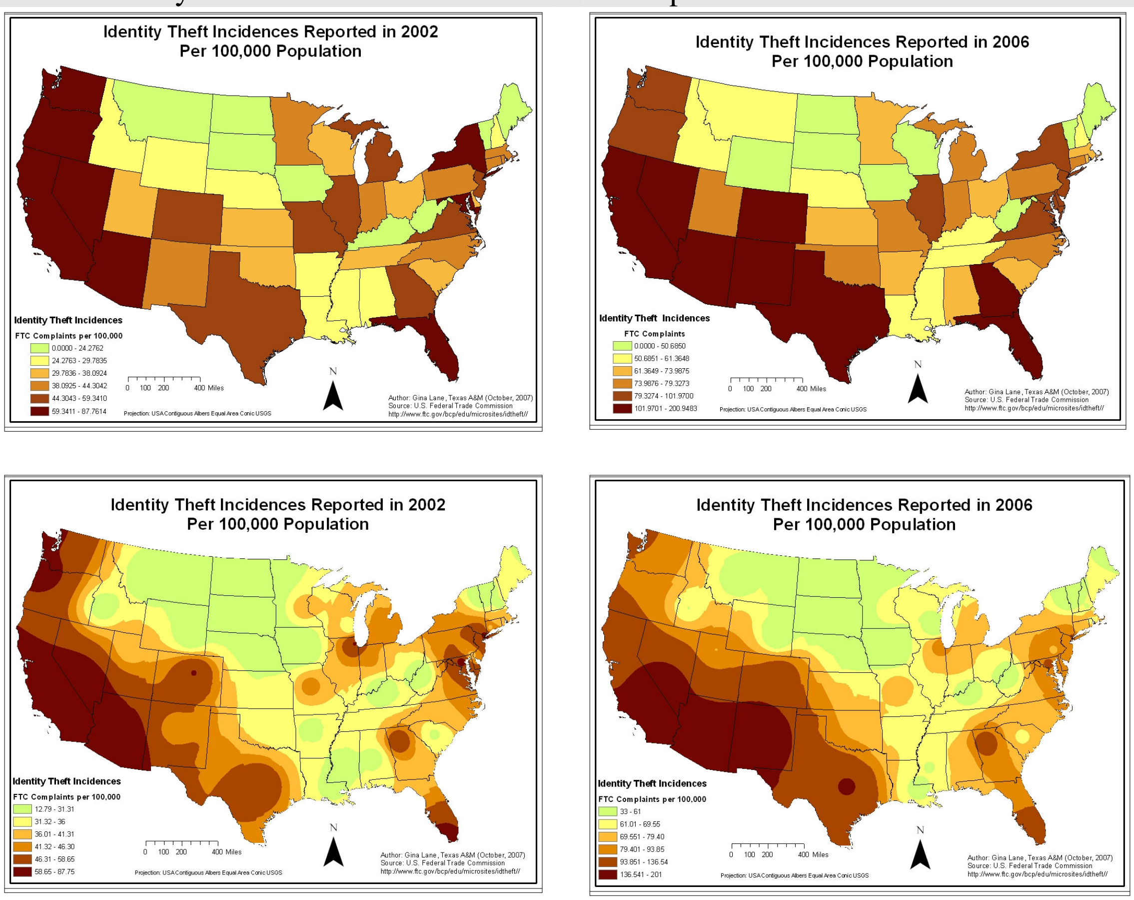

Figure 2: Comparison Maps of Identity Theft Per Capita Rates

Although most of the FTC categories show similar patterns to the overall data (some more than others), there are some regional pattern differences. In 2002, most of the FTC categories had similar per capita patterns. In particular, bank, loans, phone and utility, and credit card identity theft categories were most similar to overall 2002 per capita patterns, but employment related and government document identity theft had a more southern U.S./Mexico border concentration with much less clustering in the northern plains (Figure 3).

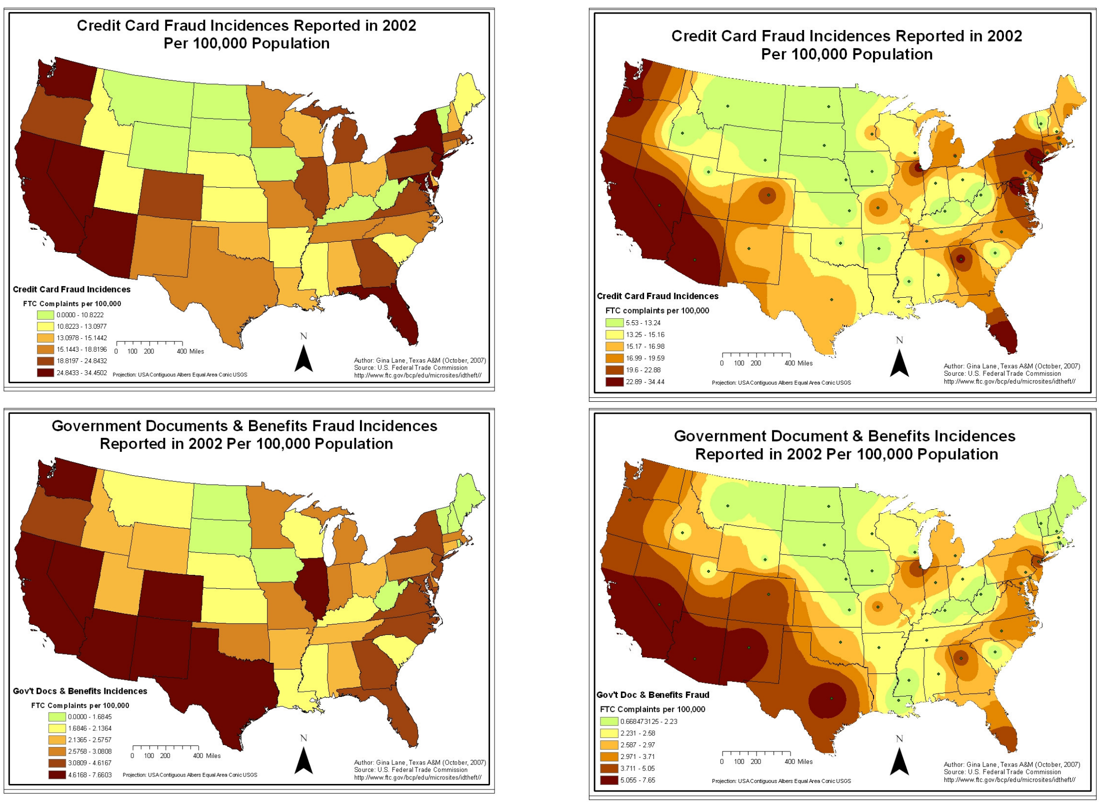

Figure 3: Spatial Patterns of Some FTC Identity Theft Categories in 2002

By 2006, the highest per capita identity theft states had shifted towards a more southern U.S./Mexico border clustering with perhaps the appearance of a southeastern cluster centered on Florida and Georgia (Figure 4). Loan, phone and utilities, and employment related identity theft patterns were remarkably similar to overall patterns, while credit card and bank related identity theft maintained dominance in west coast states, and identity theft in the form of government document fraud continued to spread across the entire southern U.S. with a clear increase in the southeast (Figure 3).

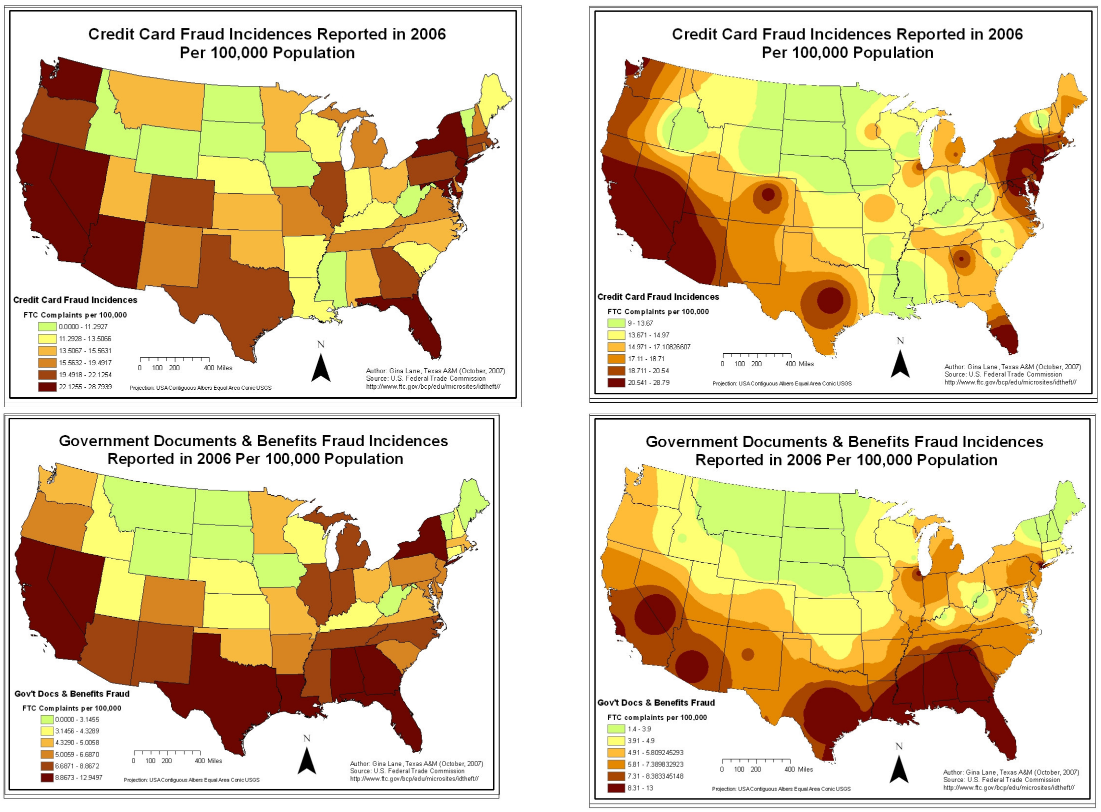

Figure 4: Spatial Patterns of Some FTC Identity Theft Categories in 2006

The spatial statistics LISA maps corroborate the patterns and clusters identified in the ArcGIS mapping, and especially illustrate the eastward shift in government document identity theft earlier identified. In 2002, a strong clustering of similar high values for per capita identity theft was confirmed for the southwestern states of CA, OR, NV, NM, and AZ. A strong clustering of similar low values for per capita identity theft was confirmed for MN, SD, and MT. By 2006, the clustering of high identity theft states expanded to include CO as well, and ND was added to the cluster of low identity theft states. By 2006, UT and OK emerged as low spatial outliers, meaning that they had relatively low rates of identity theft, yet were adjacent to neighbor states with high values.

As shown by the GIS mapping, most of the specific identity theft categories produced maps very similar to the overall identity theft rates. However, government document identity theft is particularly interesting, as it is the only category exhibiting a noteworthy geographic shift from 2002 through 2006. The LISA analysis corroborates the eastward shift identified in the ArcGIS mapping (Figure 5). Both sets of maps show a 2002 cluster of states with high identity theft rates in the form of government document and benefits fraud in the southwest states, and a cluster of states with low rates in the in the upper plains states. By 2006, a strong eastward shift had occurred, resulting in a cluster of states experiencing high government document and benefits identity theft in the southeast states, including LA, MS, AL, GA, and FL, and possibly TX. Both the ArcGIS maps and the LISA maps clearly illustrate this shift.

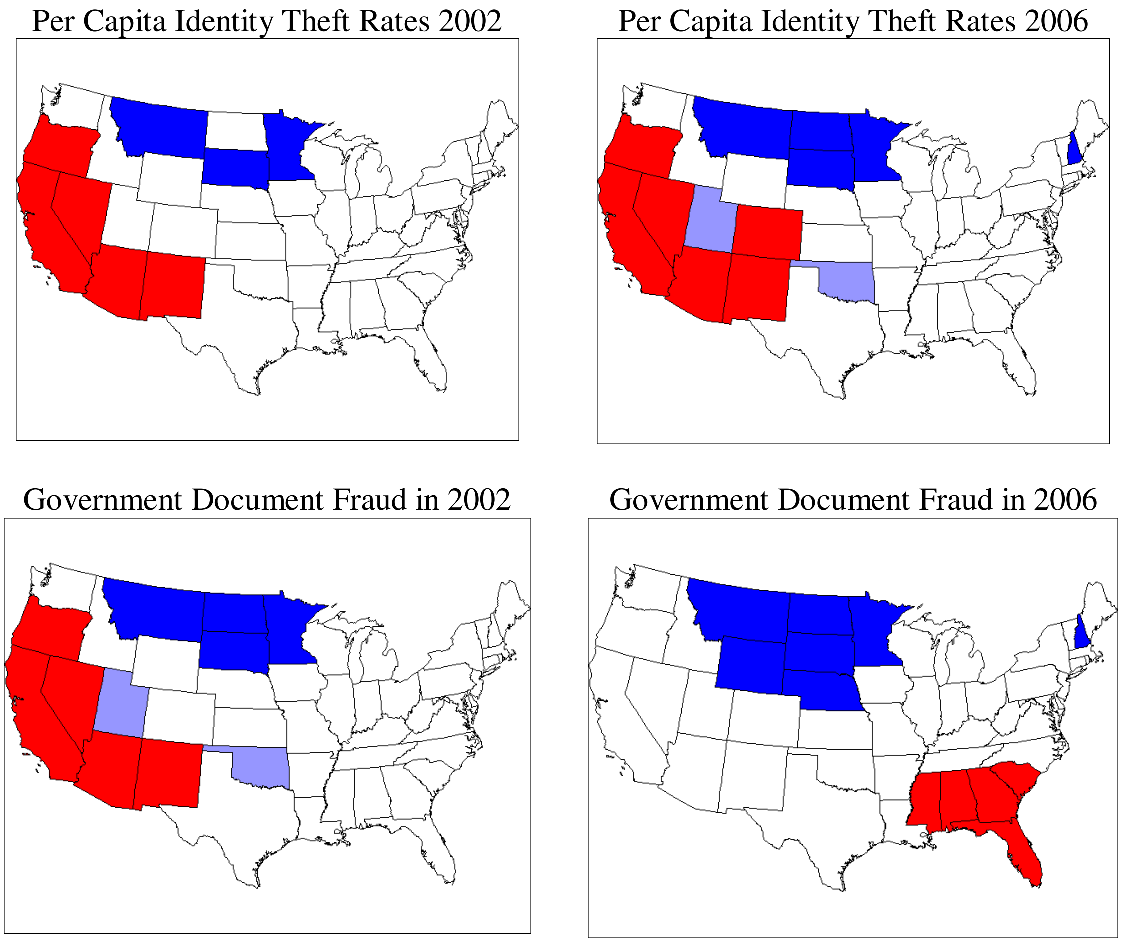

Figure 5: LISA Spatial Statistics Cluster Maps, Using Per Capita Data

4.1.2 Exploring demographic factors that may shape regional patterns

The purpose of the SPSS linear regression tests were to determine which demographic variables correlate best with the identity theft data. To do this, univariate and multivariate linear regression tests were systematically performed in order to check all demographic variables against identity theft categories. The results were successful, with some demographic variables returning correlation values (R^2) in excess of 0.700. Overall, the regression tests successfully identified which demographic variables have correlating spatial relationships to identity theft patterns (see Appendix B for complete list of results). The following paragraphs outline the general procedure performed and results for all identity theft categories in both 2002 and 2006.

In 2002, the demographic variables that returned the highest R^2 correlations with overall per capita identity theft rates were UrbanPct (.609), HISP_pct (.432), OnlinePop (.395), Est2002 (.376), DigEcon (.307), and HspFamSz (.304). Using these variables as multiple independents, the resulting multivariate model had a strong R^2 value of .753, adjusted R^2 of .719, and a p-value of .000 (recall H_o: $\beta_1 = 0$). However Est2002 and OnlinePop exhibited high collinearity. After removing Est2002 (the variable with the highest variance inflation factor or VIF), the collinearity problem was eliminated, resulting in the best multiple regression model with an R^2 of .747, adjusted R^2 of .718, and a p-value of .000. In sum, nearly 75-percent of the variance of statewide per capita identity theft rates is explained by the states' online population count, digital economy index score, hispanic family sizes, hispanic percent of the population, and percent of the population that is urban.

Similar results emerged for each of the FTC categories. For all FTC categories, the percent of population that is Hispanic (HISP_pct) showed strong R^2 values with per capita identity theft rates. In particular, employment fraud (R^2 .669), government document fraud (R^2 .697), and loan fraud (R^2 .419) had the highest correlations with Hispanic population percentages. UrbanPct and OnlinePop also consistently returned higher R^2 values for each of the FTC categories.

Following the selection of the best demographic variables for 2002, the next task is to determine whether the patterns are static or are temporally changing. To do this, the 2006 identity theft per capita data was also analyzed, using the corresponding demographic variables listed above. Whenever possible, the same demographic variables were used as the x-independents for the 2002 data. However, when available, such as with annual population estimates, 2006 data was used. Overall, the results are similar to the 2002 identity theft data, but there are some differences (Appendix 2). This may be due to the spatial shifts revealed earlier by the GIS and spatial statistics mapping. The most noteworthy change in the data, as previously mentioned, is with identity theft in the form of government document and benefits fraud. An obvious and distinct eastward shift occurred by 2006, which is largely attributed to the dramatic rise in fraudulent aid claims in the wake of Hurricane Katrina (Conkey 2007). The other FTC categories did not exhibit significant departures from the overall identity theft rates. See Appendix B for a summary of correlations for each identity theft category in 2002 and 2006.

The demographic maps help to illustrate why certain variables had higher correlations with identity theft patterns (Figure 6). For example, the concentration of some identity theft categories along the U.S./Mexico border coincides with several Hispanic variables. Not surprisingly, the states with the highest percentage of their population that is Hispanic are concentrated in the south and west along the U.S./Mexico border. There also exists a noteworthy cluster of western states with larger average Hispanic family sizes, as nationwide average Hispanic family sizes vary by up to 2:1.

Southwestern states also tend to have a much higher percent of the population that is urban. It is interesting to note that states such as Nevada and Utah, which typically are not thought of as urban, have very high urban population ratios, as most of the population lives within one or two large MSAs, and there are fewer small towns, villages, and settlements. As a result, states like Nevada and Utah are more urbanized than New York in terms of their population distributions. States with the highest digital economy index scores are clustered in the west and in New England. States with the large military barrack populations are in the southeast, plus Texas, California, and Washington. Demographic variables with less obvious spatial patterns are the number of credit issuing businesses and online population. These variables show no clear clustering of high values, but they both have some clustering of low values in the plains states, which likely explains why they returned good correlation values for some identity theft categories.

Choropleth Map of Percent Hispanic Pop LISA Cluster map of Percent Hispanic Pop

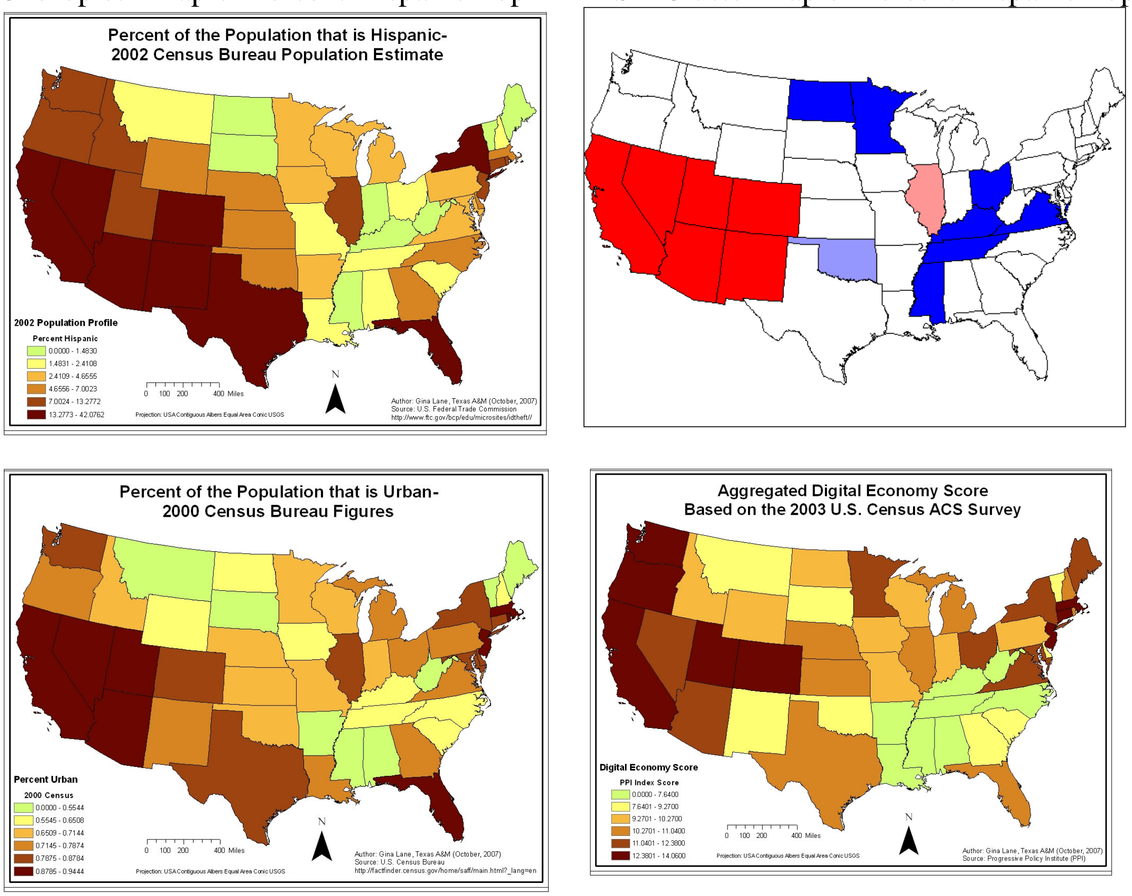

Figure 6: Spatial Patterns of Some Demographic Variables

4.2. Discussions

4.2.1 Significance of the observed regional patterns of identity theft

This study clearly illustrates the regional patterns of identity theft, which have particular significance in regards to two major rationales.

First, not only are the overall patterns of identity theft persistent from 2002 through 2006, they appear to adhere to known historic patterns for traditional larceny (theft), which leads to further insight regarding the significance of spatial patterns of crime in general. As early as the 1930s, state-level crime mapping revealed that clearly defined regional patterns existed for different crimes (measured as per capita rates) (Lottier 1938b). For example, high murder rates were concentrated in the southeastern states (FL, GA, AL, TN, AR, SC, NC, and KY). Robbery (or holdups) had particularly low rates in the New England states, and higher concentrations in the middle states (KY, TN, AR, IL, OK, CO, AZ). Most interesting, however, is that larceny, defined as the stealing of valuable property (Lottier 1938a), had remarkably similar regional patterns to recent identity theft. Lottier (1938b) discovered a western region of high larceny rates that included the states of TX, NM, AZ, NV, OR, MT, and WY. Larceny rates were low in a cluster of New England states including ME, NH, VT, NY, PA, and MA. In 1954, Shannon corroborated the persistence of these patterns in a follow up study, and by the 1970s and 1980s, crime geographers also reported the persistence of these regional patterns (Harries 1974; Herbert 1982). These studies clearly illustrate that the observed patterns had remained constant over time.

Although identity theft and larceny are fundamentally different, (larceny is considered a traditional crime while identity theft is considered a white-collar crime), they are both typically non-violent, and involve the direct theft of valuable goods from a victim. One major difference is that traditional theft is spatially dependent, because in order to steal physical property, an offender needs opportunity and proximity to do so. Despite the fact that identity theft, which many believe is increasingly occurring over the Internet, defies the need for such proximity, as a category of theft it appears to be following the patterns historically identified for traditional theft. This further illustrates that place matters in theft crime patterns, whether digital or traditional, and reemphasizes the need to identify what local factors directly contribute to theft.

Following the social ecology tradition of spatial crime studies throughout the 20th century, Lottier and Shannon rejected theories of physical determinism and proposed that crime is a societal and cultural product. Lottier (1938b) concluded that crime concentrated in urban areas, but differed regionally because of cultural differences. Lottier concluded that cities in general offered the benefit of anonymity for all criminal behavior, but that regional cultural differences are the reason for regional crime patterns. If this is true, then geographic crime patterns will continue to persist, even in cyberspace where anonymity is paramount. These cultural differences, he believed, arose as a result of differential developments in transportation, communication, agriculture, and technology. Of course, in the 1930s, no one could possibly comprehend a digital future of ubiquitous and instant communication, or modern computing capabilities. What is interesting, then, is that the observed theft patterns do appear to persist in the digital age, thus reemphasizing the potential importance of local population composition on the spatial patterns of crime. In sum, regional patterns of crime appear to be persistent in space regardless of developments in communications, transportation, and technology.

The main objective stemming from this argument is to illustrate the persistence of spatial patterns of theft crimes over time, regardless of technological developments. This is an important realization in the study of identity theft patterns, as it confirms that place remains significant, regardless of the technology used. It also provides a theoretical basis to justify further in-depth analysis of local populations. If place matters, a better understanding of the characteristics of local populations is a first step in understanding potential social characteristics associated with identity theft, and this thesis is an early attempt in achieving this goal.

The second reason the observed spatial patterns are important is in regards to the spatial shift of identity theft in the form of government document and benefits fraud. This shift is important towards this research less because of the fact that it occurred, and more because of why it occurred, and what it means. Because the shift is suspected of being directly related to the aftermath of hurricane Katrina, it is an excellent example of how crime patterns can be affected by localized conditions. Katrina created a situation where massive physical changes occurred in the landscape and in the human condition. In addition to the physical damages caused by the storm and subsequent flooding, a large-scale human migration also occurred. A chaotic period of time also presented increased opportunities for crime, which was first witnessed in the looting, theft, and violence in the immediate aftermath, and which eventually appears to have also affected some forms of identity theft. In other words, crime patterns were significantly shaped by changes in local population conditions.

Therefore, the spatial shift that exists in the identity theft data supports the hypothesis that the human condition at a specific place and time can, and does, affect the regional patterns of crime. Place, and the people who live there, are important factors.

4.2.2 Identity theft, terrorism, and homeland security

Perhaps the most critical policy arena affected by increasing knowledge of identity theft is in regards to terrorism and homeland security. Researchers have learned that identity theft and credit card fraud are primary funding and operational methods for terrorist activity in the United States. Overall, identity theft is directly connected with both domestic and international terrorism (9/11 Commission 2004; Collins 2006; Comras; 2005; Kaplan et. al 2005; O'Neil 2007; Sullivan 2004; Talbot 2005; Willox & Regan 2002). Although this study does not specifically explore policy to thwart terrorism through identity theft protection and deterrence, a better understanding of identity theft may be critical to better homeland security.

Identity theft and document fraud are universally recognized as instrumental terrorist operational tools. In all likelihood, fraud and identity theft are probably the most common tactics utilized globally by terrorists. The al Qaeda manual specifically mandates the use of falsified and stolen documents (even prescribing multiple identities per terrorist) in order to fraudulently obtain official documentation, travel, establish utilities, obtain financing, rent housing, vehicles and mail boxes, and anonymously carry out "assassination operations" (Collins 2006, p. 20). O'Neil (2007) states that "the 9/11 hijackers committed a wide variety of immigration offenses in order to enter the United States. The 19 hijackers used 364 aliases, several had fraudulently altered their passports, …[and] lied on their visa applications…" (p. 18). Sadly, there are countless examples such as these that illustrate the pervasiveness of identity theft and document fraud by terrorists who eagerly take advantage of various loopholes and systemic weaknesses in their operations and planning (Table 6). For example, as late as the mid-1990s, the Immigration and Naturalization Service (INS) was operating with outdated technology, which created an environment grossly inadequate to prevent fraudulent international asylum applicants. Terrorist watch lists were inaccurate and unenforceable throughout the 1990s, and visa processing procedures were in dire need of reform (9/11 Commission 2004).

Table 6: Known Uses of Identity Theft and Fraud by Terrorists

Individual Terrorist(s) and/or Group	Plot or Operation	Identity Theft or Fraud Activity
Ajmad Ajaj and Ramzi Yousef	1993 WTC Bombing	Illegal US immigration via document fraud
Tawfiq bin Attash (aka Khallad)	USS Cole Attack	Applied for US visa under false identification
Ramzi Binanshibh	Intended 9/11 pilot	Applied for travel documentation under fraudulent identity (Ramzi Omar)
Atta, Shehhi, Jarrad	9/11 Pilots	Falsified/obtained passports; fraudulent US visa applications
Ahmed Ressam	Foiled Y2K Bombings	Illegal immigration via document fraud, altered passport to conceal Afghan travel, illegal trafficking of passports, credit cards, and identity documents via an Islamic terrorist document broker
Hazmi and Hanjour	9/11 hijackers	Used fraudulent documents to obtain photo IDs from the New Jersey and Virginia DMV
Imam Samundra	Bali bombings	Partially financed the operation through online credit card fraud
Al Qaeda	9/11, others	Passport alteration, document fraud, identity theft

Sources: 9/11 Commission Report, 2004; Talbot 2005; Kaplan, Fang, and Sangwan 2005

It is important to note that terrorist identity theft extends far beyond the mere theft and misuse of personal information for operations support, financing, and planning. Without identity theft, terrorists may not be able to freely travel internationally, the importance of which is paramount in that:

> For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. [They accomplish this through] …altered and counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud (9/11 Commission 2004, p 384).

Not surprisingly, al Qaeda is notorious for operating organized scams to facilitate a steady supply of fraudulent/stolen documents. For example prior to 9/11, al Qaeda ran the passport office in the Kandahar airport in which they facilitated illegal terrorist travel via altering and/or falsifying travel documents, passports, visas, and identification cards. Fourteen of the 9/11 hijackers are believed to have used passports that were altered in the Kandahar office. Al Qaeda also implements 'passport collection schemes,' which involves the confiscation of passports of Northern Alliance fighters prior to deployment so that if the fighter dies, the passport can be used for someone else. In addition, the terrorists themselves (e.g. Mohamed Atta) receive specific training in document forgery to empower them to travel clandestinely and independently cover their tracks as they traverse (9/11 Commission 2004). Perhaps most shocking is the violence and brutality which al Qaeda has imposed to fraudulently obtain false identities. James Woolsey, former head of the CIA, reported that twelve of bin Laden's known terrorists had stolen the identities of western-educated men, murdered them and their entire families in order to eradicate any links back to the real individuals, and then proceeded to use the identities in global travel (Collins 2006).

Al Qaeda is not the only group known to engage in elaborate identity theft and fraud schemes, and numerous agencies actively participate in combating the problem. For example, the UN Monitoring Group reports theft rings that finance terrorist groups through identity document trafficking, stolen/forged credit cards and credit card numbers, and stolen passports (Comras 2005). Additionally, the U.S. Secret Service has included in its mission statement the investigation of "…financial crimes that include…access device fraud, financial institution fraud, identity theft, [and] computer fraud…" (US Secret Service 2007). By 2008, a special Secret Service Financial Crimes Division (FCD) had been established to investigate financial crimes specifically.

Efforts in exposing identity theft organizations have had particular successes. In 1998, for example, two terrorist groups were discovered to have stolen over $21 million from U.S. banks via credit card fraud (Sullivan 2004). In 2004, a Brooklyn couple ran an extensive identity theft ring and was suspected of terrorist connections due to incriminating possessions and a history of large money transfers to China and Turkey. During a raid of their apartment, police found over 1,000 credit card numbers, blank and forged credit cards, credit card readers, $17,000 in cash, and suspicious computer software. The couple also had 54 separate bank accounts which held up to $50,000 each (Healy 2004). Lastly, supporters of the 9/11 attacks were indicted for generating over $1 million through stolen credit cards and false identities and transferring it to Saudi Arabia via clandestine couriers to avoid detection of large electronic transfers (Sullivan 2004).

Clearly, due to the direct threat towards citizens, and the indirect threat of homeland security at the local, state, and national levels, the crime of identity theft is in dire need of more research and better understanding.

5. SUMMARY, CONCLUSIONS, AND FUTURE STUDIES

5.1. Summary

These initial assessments provide compelling evidence in support of the central hypothesis for this research, which is that regional trends exist for identity theft and that corresponding demographic variables are likely a contributing force. Using aggregate data from the FTC and U.S. Census bureau, distinct regions of varying intensities of identity theft were revealed through GIS mapping and spatial statistics analyses. By comparing 2002 and 2006 data, spatial and temporal shifts of identity theft patterns were also revealed. Social and demographic correlations were identified, such as ethnicity ratios and urban composition of the population, which may indicate that certain population subsets may be at higher risk for identity theft victimization. And lastly, the social implications of identity theft were discussed. The persistence of identity theft patterns similar to the known patterns of traditional theft indicates that place matters in crime analysis, regardless of technological advances and the introduction of cyber theft. The spatial shift of identity theft in the form of government document and benefits fraud following hurricane Katrina clearly illustrates that the location of a major catastrophe and subsequent changes in the human conditions can precipitate a spatial shift that directly affects crime patterns. And finally, a discussion of identity theft as a known facilitating method of terrorist precursor crimes revealed that identity theft creates far greater social detriment beyond the individual victims' financial and personal losses. In terms of homeland security, identity theft indirectly affects the national, perhaps even global, population.

5.2. Conclusions

This project is the first known geographic analysis of identity theft, and is also an early attempt at identifying broad demographic trends directly associated with identity theft at a national scale. This thesis observes identity theft from a general perspective, and provides a national-scale analysis of identity theft patterns in the U.S. from 2002-2006.

The results confirmed previously recognized trends such as higher rates in the southwestern states and lower rates in New England and the northern plains states. The results also revealed interesting departures from the overall trends. Although most identity theft categories were found to have similar patterns to overall identity theft, an eastern shift of government document fraud reports was identified. Speculation that this trend may be a direct result of federal aid fraud after Hurricane Katrina indicates that major events can have a dramatic effect on crime patterns. This is important, because it bolsters the argument that crime patterns are linked to the human social and demographic condition at particular locations, thus providing credence to the premise that social ecological spatial analysis of crime is an important contribution to a comprehensive body of literature regarding identity theft. It will be interesting to observe if future trends persist in the wake of Hurricane Ike or any other major national disaster.

Interestingly, identity theft appears to maintain the well-documented regional patterns of traditional larceny and theft crimes, thus indicating that geographically independent digital opportunities do not appear to eradicate the importance of place in criminal patterns. It is evident that regardless of technological means, understanding where crime happens remains important in knowing why crime happens, to whom, and by whom, even in the digital age.

Identity theft, like all crimes, is a human activity. Policy will not be effective if we do not have a comprehensive understanding of the location and characteristics of the people who are not only committing the crime, but those who are at highest risk of victimization. Geography is key in understanding the humanity of identity theft.

"[C]omputers do not steal identities… people do (Collins 2006: 181)," and until we gain a better understanding of who and where those people are, there is no real hope of slowing the progress of identity theft.

5.3. Future studies

Identity theft is a growing and evolving problem that needs a multi-faceted and multi-disciplinary approach in order to fully understand it. To date, several disciplines have engaged in nascent research into the complexity of the identity theft problem, and geographic research is an important contribution to this growing body of literature. This thesis introduces identity theft for academic geographic research, and produces enough base knowledge to help identify specific areas in need of additional research.

Although this research successfully identified broad-scale patterns for identity theft, is unable to detect detailed nuances in the data, such as specific character traits of complainants, specific hotspots, or other more precise variations within the data.

It is important to note that although numerous identity theft and demographic variables are analyzed in this research, this list is not exhaustive. This thesis does not attempt to definitively explain social causation towards identity theft behavior. Rather, it seeks to identify potential social associations that may exist, thus enabling the possibility of more narrowly focused case studies testing the broad correlations identified here. For example, a specialized study designed to examine whether identity theft patterns are categorically linked to the Hispanic population would enable researchers to further examine possible social factors that may be affecting this phenomenon. Additionally, this study specifically addresses victims; however, to fully understand the nature of identity theft, more research needs to be done on offender patterns and characteristics as well.

From this study, localized case studies are needed to determine if the regional observations exist at smaller-scales such as state, county, or local levels. Localized analyses would reveal the effects of spatial scale on identity theft patterns, and may better identify hotspots of activity. Disaggregated data would be helpful to facilitate small-scale analysis, and could be generated through surveys or cooperative local law enforcement agencies.

REFERENCES

Acohido, Byron. 2007. Use of social security number puts military at risk of ID theft. *USA Today* June 15, 2007: B1.

Allison, Stuart F.H., Schuck, Amie M., and Lersch, Kim M. 2005. Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice* 33(1): 19-29.

Anderson, Keith B. 2006. Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing* 25(2): 160-171.

Anselin, Luc. 1995. Local indicators of spatial association – LISA. *Geographical Analysis*. 27(2): 93-115.

Anselin, Luc, Cohen J., Cook, D., Gorr, W. and Tita, G. 2000. Spatial analyses of crime. Criminal Justice, Vol. 4. In *Measurement and Analysis of Crime and Justice,* ed. David Duffee, 213-262. Washington, DC.: National Institute of Justice.

Anselin, Luc. 2006. How (not) to lie with spatial statistics. *American Journal of Preventative Medicine.* 30(2S): 3-6.

Bourne, M.L.G., and Deaton, M.L. *The dynamics of identity theft: A comparison of symptomatic and systemic solutions*. Conference Proceedings of the Systems Dynamics Society. Available from: http://207.44.232.77/conferences/2005/proceed/papers/BOURN189.pdf (last accessed 20 September 2008).

Caeton, Daniel A. 2007. The cultural phenomenon of identity theft and the domestication of the world wide web. *Bulleting of Science, Technology & Society* 27(1): 11-23.

Caslon Analytics. 2008. Identity crime. From: http://www.caslon.com.au/idcrimeguide.htm (last accessed 20 August 2008).

Cheney, Julia S. 2003. Identity theft: A pernicious and costly fraud. *Federal Reserve Bank of Philadelphia Discussion Paper, Payment Cards Center.* Philadelphia: Federal Reserve Bank of Philadelphia. From: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=927415 (last accessed 30 October 2008).

Christens, P. and Speer, P. 2005. Predicting violent crime using urban and suburban densities. *Behavior and Social Issues* 14: 113-127.

CIFAS. 2004. *Deceased fraud.* From: http://www.cifas.org.uk/default.asp?edit_id=578-57 (last accessed 1 October 2008).

Cohen, J. 1941. The geography of crime. *Annals of the American Academy of Political and Social Science* 217: 29-37.

Collins, Judith M. 2006. *Investigating Identity Theft: A Guide for Businesses, Law Enforcement, and Victims.* Hoboken, NJ: John Wiley & Sons, Inc.

Computer Fraud & Security. 2008. ID theft levels rise unabated. Front matter. *Computer Fraud & Security* 2008(3): 1.

Comras, Victor. 2005. Al Qaeda finances and funding to affiliate groups. *Strategic Insights.* 4(1) 16pp. From: http://www.ccc.nps.navy.mil/si/2005/Jan/comrasJan05.asp (last accessed 8 November 2007).

Conkey, Chistopher. 2006. ID theft complaints still rising, but rate of increase slows. *The Wall Street Journal (Eastern Edition).* New York: Jan 26, 2006: D1.

Croall, Hazel. 2001. *Understanding White-collar Crime.* Crime and Justice Series: ed. Mike Maguire. Philadelphia: Open University Press.

DPS. Deceased Preference Service. 2008. From: http://www.deceasedidentityfraud.co.uk/index.htm (last accessed 20 September 2008).

Federal Trade Commission. N.D. Reference Desk. From: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/index.html. (last accessed 1 October 2008).

Federal Trade Commission. 2003. *Federal Trade Commission Overview of the Identity Theft Program.* From: http://www.consumer.gov/idtheft/pdf/ftc_overview_id_theft.pdf. (last accessed 7 July 2007).

Federal Trade Commission. 2004. *National and State Trends in Fraud & Identity Theft*: *January – December 2003*. Annual Report from the Identity Theft Data Clearinghouse. Released January 22, 2004. From: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-data.html (last accessed 15 September 2008).

Federal Trade Commission. 2005. *National and State Trends in Fraud & Identity Theft*: *January – December 2004*. Annual Report from the Identity Theft Data Clearinghouse. Released February 1, 2004. From: http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/state-data.html (last accessed 15 September 2008).

Federal Trade Commission. 2007. *Identity Theft Victim Complaint Data: Figures and Trends January 1 – December 31, 2006* [Online version]. From http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2006.pdf (last accessed 15 September 2008).

Finch, Emily. 2003. What a tangled web we weave: Identity theft and the internet. In *Dot.Cons: Crime, Deviance and Identity on the Internet,* ed. Yvonne Jewkes, 86-104. Portland, OR: Willan Publishing.

Friedrichs, David O. 2007. *Trusted Criminals: White Collar Crime in Contemporary Society*. Belmont, CA: Thomson Wadsworth.

Furnell, S. 2007. Identity impairment: The problems facing victims of identity fraud. *Computer Fraud & Security* 2007(12): 6-11.

Ganzini, L., McFarland, B., and Bloom, J. 2001. Victims of fraud: Comparing victims of white collar and violent crime. In *Crimes of Privilege: Readings in White-Collar Crime*, eds. Neal Shover and John Paul Wright, 87-95. New York: Oxford University Press.

Glaeser, Edward L. and Bruce Sacerdote. 1999. Why is there more crime in cities? *Journal of Political Economy* 107(6): 225-258.

Green, Gary S. 1993. White-collar crime and the study of embezzlement. *Annals of the American Academy of Political and Social Science* 525: 95-106.

Harries, Keith D. 1974. *The Geography of Crime and Justice.* New York: McGraw Hill.

Harries, Keith. 1988. Regional variations in homicide, capital punishment, and perceived crime severity in the United States. *Geografiska Annaler. Series B, Human Geography.* 70(3): 325-334.

Harries, Keith D. 1999. *Mapping Crime: Principle and Practice.* Washington, DC: U.S. Department of Justice, Office of Justice Programs.

Hayward, Claudia L., ed. 2004. *Identity Theft.* New York: Novinka Books.

Healy, Patrick. 2004. F.B.I. looks for terrorist link to 2 arrested in identity theft. *New York Times* 153(52869) 3 June 2004.

Herbert, D. 1982. *The Geography of Urban Crime.* New York: Longman, Inc.

Holt, T.J. 2004. The fair and accurate credit transactions act: New tool to fight identity theft. *Business Horizons.* Sep/Oct 2004 47(5): 3-6.

Hynds, L. 2003. Hi-tech crime is the "real thing." *Computer Fraud & Security* 2003(5): 4.

ID Analytics. 2007a. *U.S. Identity Fraud Rates by Geography.* February 2007 White Paper. From: http://www.idanalytics.com/whitepapers/ (last accessed 10 September 2008).

ID Analytics. 2007b. *U.S. Identity Fraud Hot Spots.* August 2007 White Paper. From: http://www.idanalytics.com/whitepapers/ (last accessed 10 September 2008).

Ingram, D.M. 2006. How to minimize your risk of identity theft. *Journal of the American Optometric Association* 77(6): 312-314.

Javelin Strategy & Research. 2006. *2006 Identity Fraud Survey Report (Consumer Version).* Released January 2006. From: http://www.javelinstrategy.com/products/AD35BA/27/delivery.pdf (last accessed 21 August 2008).

Kahn, Charles M. and Roberds, William. 2008. Credit and identity theft. *Journal of Monetary Economics* 55(2008): 251-264.

Kaplan, David E., Bay F, and Soni S. 2005. Paying for terror. *U.S. News & World Report* 00415531 5 December 2005 139(21): 40-54.

Kreuter, Eric. 2003. The impact of identity theft through cyberspace. *The Forensic Examiner.* 12(5-6): 30-35.

Liu, Lai C, Koong, Kai S., Allison, Margaret, and Wei, June. 2005. An examination of online fraud complaint occurrences. *Issues in Information Systems* 6(2): 161-167.

LoPucki, L. 2001. *Human Identification Theory and the Identity Theft Problem.* Texas Law Review 80: 89-134.

Lottier, Stuart. 1938a. Distribution of criminal offenses in metropolitan regions. *The Journal of Criminal Law, Criminology, and Police Science* 29(1): 37-50.

Lottier, Stuart. 1938b. Distribution of criminal offenses in sectional regions. *The Journal of Criminal Law, Criminology, and Police Science* 29(3): 329-344.

Lowman, John. 1986. Conceptual issues in the geography of crime: Toward a geography of social control. *Annals of the Association of American Geographers* 76(1): 81-94.

May, David A. and James E. Headley. 2004. *Identity Theft.* New York: Peter Lang Publishing, Inc.

Milne, G. R. 2003. How well do consumers protect themselves from identity theft? *Journal of Consumer Affairs* 37(2): 388-402.

Milne, G. R., Rohm, A. J., and Shalini, B. 2004. Consumers' protection of online privacy and identity. *Journal of Consumer Affairs* 38(2): 217-232.

Moye, S. 2006. Fair and accurate credit transaction act: More protection for consumers. *The Information Management Journal.* May/Jun 2006 40(3): 62-66.

Mulrean, Jennifer. 2006. *The worst states for identity theft.* MSN Money. http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P125094.asp (last accessed 6 Aug, 2008).

NDIC. 2007. National Drug Intelligence Center. *Intelligence Bulletin: Methamphetamine-Related Identity Theft.* Paper 2007-L0424-003. May 2007.

9/11 Commission. 2004. National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* New York: W.W. Norton & Company, Inc.

Newman, Graeme R. and NcNally, Megan M. 2005. *Identity Theft Literature Review.* Document submitted to U.S. Department of Justice, July 2005. From: http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf (last accessed 20 July 2007).

Norum, P. S., and Weagley, R.O. 2007. College students, internet use, and protection from online identity theft. *Journal of Educational Technology Systems* 35(1): 45-59.

O'Brien, Timothy L. 2004. Identity theft is epidemic. Can it be stopped? *New York Times* Section 3: 1, 4.

O'Neil, Siobhan. 2007. Terrorist precursor crimes: Issues and options for Congress. *CRS Report for Congress.* 24 May 2007. From: http://www.fas.org/sgp/crs/terror/RL34014.pdf (last accessed 8 November 2007).

Openshaw, S. & Taylor, P.J. 1982. The modifiable areal unit problem. In *Quantitative Geography: A British Perspective,* eds. N. Wrigley and R.J. Bennet, 60-69. Boston: Routledge and Kegan Paul.

Payne, Brian K. 2003. *Incarcerating White-Collar Offenders: The Prison Experience and Beyond.* Springfield, IL: Charles C. Thomas Publishers, Ltd.

Peet, Richard. 1975. The geography of crime: A political critique. *Professional Geographer* 28(3): 277-281.

Pemble, Matthew. 2008. Don't panic: Taxonomy for identity theft. *Computer Fraud & Security* 2008(7): 7-9.

Progressive Policy Institute. PPI Online. *The 2002 State New Economy Index: The Digital Economy*. From: http://www.neweconomyindex.org/states/2002/04_digital_01.html. (last accessed 7 September 2008).

Rafanelli, M., Bezenchek, A., & Tininini. 1996. The aggregate data problem: A system for their definition and management. *SIGMOD Record* 25(4): 8-13.

Roncek, D.W. 1993. Mapping crime: An inescapable but valuable task for intracommunity analysis. In *Questions and Answers in Lethal and Non-Lethal Violence: Proceedings of the Second Annual Workshop of the Homicide Research Working Group,* eds. C. Block and R. Block, 155-161. Washington, DC: National Institute of Justice.

Saunders, K.M. and Zucker, B. 1999. Counteracting identity fraud in the information age: The identity theft and assumption deterrence act. *International Review of Law, Computers, and Technology* 13(2): 183-192.

Shannon, Lyle W. 1954. The spatial distribution of criminal offenses by state. *The Journal of Criminal Law, Criminology, and Police Science* 45(3): 264-273.

Slosarik, Katherine. 2002. Identity theft: An overview of the problem. *The Justice Professional* 15(4): 329-343.

Snook, B., Cullen, R.M., Mokros, A., and Harbort, S. 2005. Serial murderers' spatial decisions: Factors that influence crime location choice. *Journal of Investigative Psychology and Offender Profiling* 2: 147-164.

Stana, Richard M. 2004. Identity Theft: Prevalence and Cost Appear to be Growing. In *Identity Theft*, ed. Claudia Hayward, 17-72. New York: Novinka Books.

Sullivan, Bob. 2004. *Your Evil Twin: Behind the Identity Theft Epidemic.* Hoboken, NJ: John Wiley & Sons, Inc.

Sutherland, Edwin H. 1940. White-collar criminality. *American Sociological Review* 5 (1): 1-12.

Synovate. 2003. *Identity Theft Survey Report.* Prepared for the Federal Trade Commission. From: www.ftc.gov/os/2003/09/**synovatereport**.pdf (last accessed 3 September 2008).

Talbot, David. 2005. Terrors server: Fraud, gruesome propaganda, terror planning: The net enables it all. *Technology Review* 108(2): 46-52.

Tobler, Waldo. 1970. A computer movie simulating urban growth in the Detroit region. *Economic Geography* 46. Supplement: Proceedings. International Geographical Union. Commission on Quantitative Methods (June, 1970): 234-240.

United States 105th Congress. 1998. *Identity Theft and Assumption Deterrence Act of 1998* (H.R. 4151,EH; S.512.ES). United States 105th Congress, 2d session. Washington, DC.

US Secret Service. 2007. *Mission Statement*. From: http://www.treasury.gov/usss/mission.shtml (last accessed 15 November 2007).

Weicher, N. 2007. Educating students about ID theft. *Business Week Online* 5/9/2007: 28.

Welborn, Angie A. 2004. Identity Theft: An Overview of Proposed Legislation. In *Identity Theft*, ed. Claudia Hayward, 1-16. New York: Novinka Books.

Willox, N., and Regan, T. 2002. Identity fraud: Providing a solution. *Journal of Economic Crime Management* 1(1): 1-14.

APPENDIX A

LITERATURE-GUIDED DEMOGRAPHIC VARIABLES SELECTED FOR CORRELATION TESTING

Variable	**Definition**
Economic Indicator Variables	
CredIssu	Number of businesses issuing credit, including credit card issuing, sales financing, and other non-depository credit intermediation
CredPerCp	Statewide per capita number of credit issuing businesses, per 100,000 population, based on 2002 economic data and 2002 population estimates
DigEcon	Aggregated digital economy score. Produced by the Progressive Policy Institute (PPI) in the State New Economy Index, using 7 indicators to mreasure statewide progress to the Digital Economy (based on Census ACS 2003 Survey)
OnlinePct	Statewide percentage of population with internet access (based on Census 2003 ACS)
OnlinePop	Online population, calculated by multiplying 2003 estimated population by online percent values from the Census 2003 ACS
Family Size Data (by Race)	
AsnFamSz	Average statewide family size, head of household Asian, Census 2000
AvgFamSz	Average statewide family size, all races, Census 2000
BlkFamSz	Average statewide family size, head of household black, Census 2000
HspFamSz	Average statewide family size, head of household Hispanic, Census 2000
IslFamSz	Average statewide family size, head of household Pacific Islander, Census 2000
NatFamSz	Average statewide family size, head of household Native American, Census 2000
WhtFamSz	Average statewide family size, head of household white, Census 2000
General Statewide Population Data	
Est2002	Statewide U.S. Population Estimate for July 1, 2002
Est2006	Statewide U.S. Population Estimate for July 1, 2006
DormPop	Statewide population living in college dorms, Census 2000
MilBarak	Statewide population living in military group quarters, Census 2000
Rural2000	Total statewide rural population counts from 2000 Census
RuralPct	Percent of Census 2000 statewide population that is rural
Urban2000	Total statewide urban population counts from 2000 Census. Total urban equals the urban area population plus cluster population
UrbanPct	Percent of Census 2000 statewide population that is urban

Variable	Definition
Racial Data	
AmI2KPct	Percent of state population that is Native American in Census 2000
Asn2KPct	Percent of state population that is Asian in Census 2000
Blk2KPct	Percent of state population that is black in Census 2000
HISP_Pct	Percent of Statewide Population that is Hispanic, Census 2000
HspPct06	Percent of estimated 2006 population that is Hispanic
HspEst02	Statewide Hispanic population estimate for July 1, 2002
HspEst06	Statewide Hispanic population estimate for July 1, 2006
PcI2KPct	Percent of state population that is Pacific Islander in Census 2000
Up2pct2K	Percent of population that is two or more races in Census 2000
WhtPct2k	Percent of state population that is white in Census 2000

APPENDIX B

SPSS REGRESSION ANALYSIS RESULTS – SELECTED DEMOGRAPHIC (X) VARIABLES FOR EACH IDENTITY THEFT (Y) VARIABLE

Summary of SPSS Results in Selecting the Best Demographic Variables

Variable	**Definition**	**R^2**	**P-value**
For Y = PerCap02 (2002 ID Theft Per Capita)			
X1 = OnlinePop	Online population	.395	.000
X2 = HspFamSz	Average family size, household head Hispanic	.304	.000
X3 = DigEcon	Digital economy index score	.307	.000
X4 = HISP_pct	Percent of population that is Hispanic	.432	.000
X5 = UrbanPct	Percent of population that is urban	.609	.000
Multiple Regression	R^2 .753, Adjusted R^2 .719, p-value .000, no collinearity		
For Y = CCpcap02 (Credit Card Fraud Per Capita)			
X1 = HISP_pct	Percent of population that is Hispanic	.275	.000
X2 = UrbanPct	Percent of population that is urban	.587	.000
X3 = DigEcon	Digital economy index score	.277	.000
X4 = OnlinePop	Online population	.368	.000
Multiple Regression	R^2 .662, Adjusted R^2 .624, p-value .000, no collinearity		
For Y = GovPcp02 (Government Document Fraud Per Capita)			
X1 = OnlinePop	Online population	.400	.000
X2 = HspFamSz	Average family size, household head Hispanic	.286	.000
X3 = DigEcon	Digital economy index score	.201	.001
X4 = HISP_pct	Percent of population that is Hispanic	.697	.000
X5 = UrbanPct	Percent of population that is urban	.451	.000
X6 = HspEst02	Hispanic population estimate for July 1, 2002	.434	.000
X7 = MilBarak	Population living in military group quarters	.311	.000
X8 = CredIssu	Number of credit issuing businesses	.381	.000
Multiple Regression	R^2 .834, Adjusted R^2 .806, p-value .000, no collinearity		
For Y = EmpPcp02 (Employment Related Fraud Per Capita)			
X1 = HspFamSz	Average family size, household head Hispanic	.214	.001
X2 = HspEst02	Hispanic population estimate for July 1, 2002	.359	.000
X3 = HISP_pct	Percent of population that is Hispanic	.669	.000
Multiple Regression	R^2 .718, Adjusted R^2 .700, p-value .000, no collinearity		
For Y = LnPcap02 (Loan Fraud Per Capita)			
X1 = OnlinePop	Online population	.382	.000

Variable	Definition	R^2	P-value
X2 = HspFamSz	Average family size, household head Hispanic	.225	.001
X3 = HISP_pct	Percent of population that is Hispanic	.419	.000
X4 = UrbanPct	Percent of population that is urban	.495	.000
X5 = HspEst02	Hispanic population estimate for July 1, 2002	.295	.000
X6 = MilBarak	Population living in military group quarters	.242	.000
Multiple Regression	R^2 .699, Adjusted R^2 .657, p-value .000, no collinearity		
For Y = BnPcap02 (Bank Fraud Per Capita)			
X1 = OnlinePop	Online population	.226	.000
X2 = HspFamSz	Average family size, household head Hispanic	.333	.000
X3 = DigEcon	Digital economy index score	.242	.000
X4 = HISP_pct	Percent of population that is Hispanic	.373	.000
X5 = UrbanPct	Percent of population that is urban	.427	.000
X6 = MilBarak	Population living in military group quarters	.232	.000
Multiple Regression	R^2 .627, Adjusted R^2 .575, p-value .000, no collinearity		
For Y = PUpcap02 (Phone and Utilities Fraud Per Capita)			
X1 = OnlinePop	Online population	.378	.000
X2 = HspFamSz	Average family size, household head Hispanic	.291	.000
X3 = DigEcon	Digital economy index score	.232	.000
X4 = HISP_pct	Percent of population that is Hispanic	.216	.001
X5 = UrbanPct	Percent of population that is urban	.508	.000
Multiple Regression	R^2 .834, Adjusted R^2 .806, p-value .000, no collinearity		

Summary of SPSS Results with 2006 Identity Theft Data

Variable	Definition	R^2 value	P-value
For Y = PerCap06 (2006 ID Theft Per Capita)			
X1 = OnlinePop	Online population	.180	.002
X2 = HspFamSz	Average family size, household head Hispanic	.159	.004
X3 = DigEcon	Digital economy index score	.108	.020
X4 = HISP_pct	Percent of population that is Hispanic	.782	.000
X5 = UrbanPct	Percent of population that is urban	.359	.000
Multiple Regression	R^2 .795, Adjusted R^2 .781, p-value .000, no collinearity		

Variable	**Definition**	**R^2 value**	**P-value**
For Y = CCpcap06 (Credit Card Fraud Per Capita)			
X1 = HISP_pct	Percent of population that is Hispanic	.381	.000
X2 = UrbanPct	Percent of population that is urban	.622	.000
X3 = DigEcon	Digital economy index score	.344	.000
X4 = OnlinePop	Online population	.385	.000
Multiple Regression	R^2 .715, Adjusted R^2 .689, p-value .000, no collinearity		
For Y = GovPcp06 (Government Document Fraud Per Capita)			
X1 = OnlinePop	Online population	.308	.000
X2 = DigEcon	Digital economy index score	.005	.611
X3 = HISP_pct	Percent of population that is Hispanic	.228	.000
X4 = UrbanPct	Percent of population that is urban	.164	.004
X5 = HspEst06	Hispanic population estimate for July 1, 2002	.199	.001
X6 = MilBarak	Population living in military group quarters	.174	.003
X7 = CredIssu	Number of credit issuing businesses	.458	.000
Multiple Regression	R^2 .726, Adjusted R^2 .681, p-value .000, no collinearity		
For Y = EmpPcp06 (Employment Related Fraud Per Capita)			
X1 = HspFamSz	Average family size, household head Hispanic	.154	.005
X2 = HspEst06	Hispanic population estimate for July 1, 2002	.196	.001
X3 = HISP_pct	Percent of population that is Hispanic	.515	.000
X4 = RuralPct	Percent of population that is rural	.184	.002
Multiple Regression	R^2 .548, Adjusted R^2 .508, p-value .000, no collinearity		
For Y = LnPcap06 (Loan Fraud Per Capita)			
X1 = OnlinePop	Online population	.269	.000
X2 = HspFamSz	Average family size, household head Hispanic	.199	.001
X3 = HISP_pct	Percent of population that is Hispanic	.587	.000
X4 = UrbanPct	Percent of population that is urban	.445	.000
X5 = HspEst06	Hispanic population estimate for July 1, 2002	.283	.000
X6 = MilBarak	Population living in military group quarters	.167	.003
Multiple Regression	R^2 .696, Adjusted R^2 .654, p-value .000, no collinearity		

Variable	**Definition**	**R^2 value**	**P-value**
For Y = BnPcap06 (Bank Fraud Per Capita)			
X1 = OnlinePop	Online population	.223	.001
X2 = DigEcon	Digital economy index score	.197	.001
X3 = HISP_pct	Percent of population that is Hispanic	.495	.000
X4 = UrbanPct	Percent of population that is urban	.343	.000
Multiple Regression	R^2 .555, Adjusted R^2 .516, p-value .000, no collinearity		
For Y = PUpcap06 (Phone and Utilities Fraud Per Capita)			
X1 = OnlinePop	Online population	.007	.551
X2 = HspFamSz	Average family size, household head Hispanic	.000	.907
X3 = DigEcon	Digital economy index score	.001	.884
X4 = HISP_pct	Percent of population that is Hispanic	.421	.000
X5 = UrbanPct	Percent of population that is urban	.045	.862
Multiple Regression	R^2 .502, Adjusted R^2 .806470, p-value .000, no collinearity		

VITA

Gina W. Lane received her Bachelor of Science degree in geography from Texas A&M University, College Station in 1993. Her professional background includes merchandising, operations development, and management for Wal-Mart Stores, Inc., real estate, and MPO urban/transportation planning. She entered the Graduate Studies program at Texas A&M University in August 2005, and received her Master of Science degree in December 2008. Her research interests include GIS, demographics, crime study, and social geography.

Gina Lane may be reached at gnmlane@suddenlink.net.