Spring 2024

Cybercrime Victimization: Online Routine Behaviors, Guardianship, and Identity Theft Victimization in a Nationally Reflective Sample

Ifeoluwa Stella Elegbe

CYBERCRIME VICTIMIZATION: ONLINE ROUTINE BEHAVIORS, GUARDIANSHIP, AND IDENTITY THEFT VICTIMIZATION IN A NATIONALLY REFLECTIVE SAMPLE

by

IFEOLUWA S. ELEGBE

Under the direction of Adam Bossler

ABSTRACT

In this digital era, cybercrime victimization has emerged as a significant issue, with identity theft being one of the most prevalent forms. This study examines the relationship between online routine behaviors, guardianship, demographics, and identity theft victimization in a nationally representative sample of U.S. adults utilizing routine activities theory (RAT) as a conceptual framework. The research applies statistical methods such as descriptive statistics, correlation analysis, and logistic regression models to examine theoretically oriented hypotheses. The hypotheses suggest connections between different online habitual behaviors, steps taken to protect oneself, demographic characteristics, and the extent to which one has been a victim of identity theft. Surprisingly, the results indicate that spending more time browsing the Internet was related with higher levels of identity theft victimization. Increased usage of social media was not related with identity theft victimization. Other online activities, however, such as engaging in online shopping, utilizing cryptocurrency, and exploring the Dark web were related with higher levels of victimization. In contrast to routine activities theory, higher levels of online guardianship were related with higher levels of identity theft victimization, indicating that post-victimization practices may be influencing this association. Except for age, demographic characteristics had minimal correlation with victimization. Older persons had a decreased likelihood of encountering identity theft, maybe attributable to their less technological expertise

or more cautious online practices. The study emphasizes the need of using the Routine Activities Theory (RAT) as a framework to analyze cybercrime victimization. It also emphasizes the necessity of developing specific solutions based on empirical research. The study acknowledges limitations, such as the use of a cross-sectional design and the representativeness of the sample. It highlights the need for future research to include longitudinal data and more precise measuring methods. In summary, this study adds to the ongoing discussion on cybercrime victimization and provides insights for developing preventative and intervention methods to safeguard persons from identity theft in the digital world.

INDEXWORDS: Cybercrime, Identity theft, Routine activity theory, Guardianship, Online behaviors, and Victimization, Cybersecurity, Unauthorized, Cryptocurrency, Personal Information.

CYBERCRIME VICTIMIZATION: ONLINE ROUTINE BEHAVIORS, GUARDIANSHIP, AND IDENTITY THEFT VICTIMIZATION IN A NATIONALLY REFLECTIVE SAMPLE

By

IFEOLUWA S. ELEGBE

LL.B., Ekiti State University, Nigeria, 2019

M.Sc., Georgia Southern University, 2024

A Thesis Submitted to the Graduate Faculty of Georgia Southern University in Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

CYBERCRIME VICTIMIZATION: ONLINE ROUTINE BEHAVIORS, GUARDIANSHIP, AND IDENTITY THEFT VICTIMIZATION IN A NATIONALLY REFLECTIVE SAMPLE

by

IFEOLUWA S. ELEGBE

Major Professor:	Adam Bossler
Committee:	Cassandra Dodge
	Logan Somers

Electronic Version Approved:

May 2024

DEDICATION

I dedicate this thesis to God, for His guidance, gift of life, grace, and blessings, which have illuminated my path with clarity and purpose, and provided me with strength and wisdom throughout my academic journey. (Psalm 63:7).

I dedicate this thesis to my mum (Folawewo Elegbe); I am forever grateful to God for your unwavering presence in my life. Your sacrifices, and encouragement have shaped my path and fueled my determination to excel. May this thesis serve as a testament to the profound impact of your love and support on my life and academic pursuits.

ACKNOWLEDGMENTS

I am deeply grateful to my supervisor Dr.Adam Bossler for his unwavering effort, time, and guidance in helping me reach this milestone. His dedication, support and expertise are truly commendable, and I feel incredibly fortunate to have the opportunity to work under his guidance, thank you! I extend my sincere appreciation to my thesis committee Dr Cassandra Dodge and Dr Logan Somers for their thoughtful insights, scholarly guidance, and critical evaluation of this thesis. I am profoundly thankful for their generous investment of time and effort in ensuring the success of this endeavor.

I would like to acknowledge and say a big thank you to Georgia Southern University, Dr. Chad Posick, Dr. Aki Dawson, Dr. Kristina Thompson, and my uncle (Mr Musibau Fasaye).

To my beloved family, I offer my heartfelt my appreciation to my Parents and my awesome siblings for their boundless love, patience, and encouragement throughout this journey.

Lastly, to my friends and loved ones who have stood by me with patience and encouragement, thank you!

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

The Federal Trade Commission (FTC) has shown a significant increase in the occurrence of identity theft, with more than 5.7 million incidents reported in 2021, highlighting the pressing requirement for efficient solutions (Federal Trade Commission 2022). In 2015, the United States announced that a massive data breach occurred regarding records retained by the United States Office of Personnel Management (OPM). Although initially thought to *only* affect four million federal employees, it was later found that the breach affected over twenty million (22.1) individuals as it affected federal employees, individuals who went through federal background checks, and their friends and family as well. Data that was breached included, but were not limited to, Social Security numbers, dates of birth, and places of birth. This breach is considered one of the largest data breaches that affected the U.S. government in its history. The suspected criminals were not individual hackers, but instead were believed to be the Jiangsu State Security Department, an advanced persistent threat located in China. The total damage inflicted by this data breach is still unknown to this day (Fruhlinger, 2020; OPM, n.d.) Furthermore, the COVID-19 epidemic increased adaptation to remote employment and online activities, hence intensifying the vulnerability to cybercrime victimization. The rise in remote work and internet activities has greatly amplified the risk of encountering cybercriminals (Europol 2020).

In addition to this massive data breach, the occurrence of several other prominent data breaches in the twenty-first century, involving well-known entities

like Equifax, Yahoo, and Anthem, has prompted scholars (e.g., Allison, Schuck, & Lersch, 2005; Burnes et al., 2020; Harrell, 2019; Reyns, 2018) to examine the potential influence of individual-level characteristics and behaviors on the risk of becoming victims of identity theft. Personal information maintained or stored online can be compromised by cybercriminals through the utilization of phishing techniques, vulnerabilities in computer systems, and malware (Holt, Bossler, & Seigfried-Spellar, 2022). The widespread adoption of online shopping, banking, and social media has also led to a rise in the exchange of personal information, facilitating cybercriminals and hackers in obtaining sensitive or crucial data (Cavusoglu, 2004). This escalation in cybercrime has led to an erosion of public confidence in digital transactions and online platforms (Kshetri, 2010).

Identity theft has become an important concern for business organizations, institutions, and individuals alike. Identity theft is the most rapidly expanding criminal activity in the United States (Federal Trade Commission, 2021). This upward trajectory is largely propelled by technological advancements and the widespread use of the Internet. The emergence of new technologies leads to more crimes as cybercriminals are continuously developing novel techniques to take advantage of vulnerabilities to execute a wide range of cyber offenses.

In this thesis, I contribute to the literature on identity theft victimization by using a routine activities theory framework (Cohen and Felson, 1979) to examine the relationship between online routine behaviors, such as browsing the Internet and online shopping, protecting oneself online (i.e. guardianship), and demographics with identity theft victimization in a nationally reflective sample. Based on a review of the literature, it is hypothesized that individuals who spend more time online, including browsing the Internet, using social media, purchasing items online, using

cryptocurrency, and surfing the dark web, will be more likely to be victims of identity theft victimization. In addition, it is hypothesized that individuals with higher levels of online guardianship (e.g., changing passwords, etc.) will have lower levels of identity theft victimization. Finally, based on the conflicting evidence in the literature, it is hypothesized that there will be no significant relationships between demographics (e.g., sex, race, ethnicity, income, education, etc.) and identity theft victimization.

CHAPTER 2

LITERATURE REVIEW

Defining Identify Theft

The definition of identity theft varies among scholars and government reports (e.g., Federal Trade Commission, 2021; U.S. Department of Justice, 2021). Accepted definitions of identity theft commonly revolve around the unauthorized utilization of personal information. Personal information commonly encompasses an individual's name, Social
Security number, credit card particulars, bank account details, and other distinctive data (Federal Trade Commission, 2021). The illicit or illegal utilization of such data is an inherent characteristic of identity theft, irrespective of the particular circumstances or techniques employed.

According to the United States Department of Justice (2021), identity theft refers to the illegal acquisition of an individual's personal information, typically by fraudulent or deceitful methods or means, with the aim of obtaining financial and economic benefits. The act of obtaining anything illegally is a major problem, as it brings attention to the basic elements of identity theft and the necessity for more stringent rules (U.S. Department of Justice, 2021).

National Crime Victimization Survey Identity Theft Supplement

The Bureau of Justice Statistics (BJS), a division of the US Department of Justice, is a body that helps in gathering or collating, compiling, processing, or analyzing data for statistical purposes (Bureau of Justice Statistics, 2021). The National Crime Victimization Survey (NCVS) started in 1973 and is the primary

source of data on criminal victimization in the United States. The NCVS has conducted a few supplemental reports on identity theft victimization. The Identity Theft Supplements includes three general types of incidents in its definition of identity theft: (1) unauthorized use or attempted use of an existing account; (2) unauthorized use or attempted use of personal information to open a new account; and (3) misuse of personal information for a fraudulent purpose. Victims who report having experienced any incidents of identity theft in the last 12 months are questioned about the incident and how they handled it, including how they discovered the theft, any problem or loss it caused, duration of time it took them to fix those problems, and whether they reported the theft to the police and credit bureaus (Bureau of Justice Statistics, 2021). The supplemental report requests information on the total financial losses suffered as a result of all incidents from victims who reported having multiple instances of identity theft during the year. Additionally, it queries respondents on their experiences with identity theft outside of the reference period and the security precautions they took (Bureau of Justice Statistics, 2021).

Scope of Problem

According to the Internet Crime Complaint Center (IC3), which is operated by the Federal Bureau of Investigation (FBI), the IC3 received approximately 51,000 reports of identity theft in 2021, resulting in $278 million in losses for the United States economy (Internet Crime Complaint Center, 2022). This is clearly a significant underrepresentation of how much identity theft and online fraud exists as these reports only consist of reported identity theft. In 2021, Delaware, Florida, and Kentucky had the highest per capita rates of identity theft and fraud. Additionally,

Georgia, Nevada, Maryland, Louisiana, and Rhode Island recorded the highest number of cases of fraud and identity theft (Federal Trade Commission, 2022). Identity theft represented 25% of all reported incidents in 2021, while Imposter Scams accounted for 17.2%.

According to the 2018 Identity Theft Supplement of the National Criminal Victimization Survey, approximately 9% of 23 million individuals had been victims of identity theft in that past 12 months (Harrell, 2021). The crimes they experienced included several forms of victimization, including misuse of credit cards, personal information, and bank accounts. Five percent experienced identity theft through the misuse or appropriation of their credit card, 4% were involved in the misuse of their existing bank account, and 1% experienced the misuse of their personal information for other fraudulent purposes (Harrell, 2021). Less than 1% of the respondents had someone open up a new account in their name without their authorization.

In addition to the growing incidence of identity theft, there exists a developing comprehension of the adverse emotional and physical health implications associated with financial crimes. Approximately 10% of those who fell victim to identity theft, amounting to approximately 2.6 million individuals, experienced significant psychological distress as a consequence of their victimization (Harrell, 2019). Furthermore, according to Sharp et al. (2004), a study revealed that a significant proportion, specifically 25%, of individuals who fell victim to Identity theft experienced sleep disturbances, anxiety, and irritability for a duration of six months following the occurrence.

The financial impact of identity theft victimization is not equally felt by all demographics. Reynolds's (2021) examination of the 2016 Identity Theft Supplement found that being Hispanic and having a good education were important

predictors of enduring outof-pocket losses because of identity theft (Reynolds, 2021). The chance of financial losses rose with age, lower income, lower education, single status, and Hispanic/Latinx ethnicity. The findings of this research raise questions about the widely held belief that higher-income people are more vulnerable to identity theft (Reynolds, 2021). Instead, data demonstrates that lower-income persons have a greater financial effect and are more likely to suffer personal financial losses because of identity theft.

In addition, the emotional pain of identity theft victimization is not felt equally among all victims. Golladay and Holtfreter's (2017) examination of the Identity Theft Supplement to the National Crime Victimization Survey found greater levels of mental and physical suffering related with more recent victimizations of identity theft victimization. In fact, age, minority status, and the amount lost were similarly connected to heightened emotional repercussions. Higher income and education levels, on the other hand, were linked to lower levels of emotional discomfort. These results offer insight into the emotional consequences, and not just the financial consequences, of the impact of identity theft victimization on U.S. citizens.

General Background Information on Identity Theft

Identity theft has been an important concern for a much longer period of time than simply since the advent of the Internet era. According to Irshad and Soomro (2018), the rise of identity theft is shown through many periods, beginning as far back as the 1800s. For example, from 1800 to 1918, outlaws murdered individuals and usurped their identities. From 1919-1921, numerous instances of voter fraud occurred when individual'' identities were taken in order to cast substantial numbers

of votes. In addition, adolescents have fabricated counterfeit identification documents in order to purchase alcoholic beverages going back to at least 1931. The introduction of credit cards in the 1960s provided criminals with additional avenues for engaging in identity theft. With the proliferation of technology in the 1990s, identity theft saw a sharp increase. The advent of the Internet and search engines such as Google prompted individuals to disclose personal information. Therefore, in the early 2000s, credit reporting companies were directed to furnish credit records to customers in order to mitigate the risk of fraudulent accounts being established. Later, the National Crime Victimization Survey was finally enhanced to incorporate novel manifestations of Identity Theft (Irshad & Soomro, 2018).

Identity theft has been a prevailing consumer complaint for more than 15 years (Burnes et al., 2020). As a result of heightened security measures implemented by American banks, thieves have resorted to alternative venues for perpetrating identity theft. The rapid advancement of technology has led to the introduction of new applications, which unfortunately has provided thieves with increasingly greater opportunities to access personal information. According to Burners et al (2020), the numerous high-profile data breaches occurring throughout the twenty-first century raises the question of whether individual-level characteristics and behaviors contribute to the risk of identity theft victimization.
Additionally, the question arises as to whether victimization risk is primarily dependent on business and government data security procedures.

The methods of identity theft have even changed over the last few decades. Criminals used to resort to “"dumpster diving”" in which criminals physically combed through trash bins for abandoned invoices and papers holding personal information. Another traditional or old-fashioned technique of identity theft is

“"shoulder surfing”" to gain credit card or calling card numbers, eavesdropping on conversations to obtain PINs, and recovering abandoned mail with credit card pre-approval applications (Brooks, 2003; The United States Department of Justice, 2017). Solove (2004) proposes that identity theft has developed alongside the progression of technology, embracing not only traditional or old-fashioned forms of fraud, but also cybercrimes that take advantage of vulnerabilities in online structures.

Phishing is a recent cybercrime method where criminals employ false emails or fake websites to trick consumers into revealing sensitive information like Social Security numbers, date of birth, security, or login passwords. Another method frequently used by identity thieves is “skimming”, where criminals install devices on ATMs or point-of-sale terminals to capture credit card information. In a recent case, a gang of identity thieves in California installed skimming devices in gas stations resulting in the theft of thousands of credit card details. The criminal and his co-conspirators captured at least 8,229 stolen card numbers, resulting in an estimated loss of $5,032,616. The investigation of the case was conducted by the United States Secret Service in collaboration with Assistant U.S. Attorney Eric Schmale (U.S. Attorney’s Office, 2023).

In addition, there are multiple forms of identity theft according to the United States Identity Theft Resource Center (Allison, Schuck et al., 2005). Each of these categories involves a cybercriminal using personal information without the victim’s knowledge with the intention of committing a crime by using the information. Financial identity theft entails bank account and credit card fraud, giving victims significant financial stress. Opening new accounts in the victim’s name, altering mailing addresses, and opening new bank accounts are some of the techniques used.

Identity theft has also emerged as a major issue in recent years in the medical field, where criminals exploit pilfered personal data or information to acquire medical treatments or insurance reimbursements (Seh et al., 2020). Medical identity theft entails utilizing personal information such as a person's name and Medicare number to purchase medical supplies, prescriptions, or present bogus billings, causing major problems, altering credit scores, and possibly jeopardizing medical records. Identity theft can also involve fraudulent utilization of another individual’s Social Security number (SSN) for the purpose of claiming a tax return, resulting in the victim being unaware of the theft (Taxpayer Guide to Identity Theft | Internal Revenue Service, n.d.)

CHAPTER 3

THEORETICAL FRAMEWORK

Lawrence Cohen and Marcus Felson presented routine activities theory (RAT) in 1979, which connected recurring patterns of everyday living to changes in the crime rate in the United States (Cohen and Felson, 1979). RAT states that when motivated criminals come across satisfactory or suitable targets without adequate guardianship, criminal activity is more likely to occur. Instead of focusing on the reasons why criminals commit crimes, it considers the situations in which they will behave. The theory defines motivated offenders as individuals who are more exposed to and close to prospective targets, which increases their likelihood of victimization. Those who are suitable targets are more likely to become victims of crime, as well as unprotected or negligently guarded targets, who likewise face a higher chance of victimization (Cohen and Felson, 1979).

When RAT was first developed by Cohen and Felson in 1979, it was mainly intended to explain conventional crimes that took place in real or physical locations (Reyns, 2018). RAT is an often-referenced theory in criminology that explains crime and victimization. It is still unclear if the theory can be used to explain how cybercrime unfolds since it was created before the Internet fundamentally altered everyday life routines.

The key hypotheses of the theory have often been validated by research. The results of exposure, suitable target, and guardianship often match up with predictions from theory (Reyns, 2018). A variety of outcomes, such as criminal behavior,

deviance, and different forms of criminal victimization, such as sexual victimization and identity theft, have found support for RAT hypotheses (Reyns, 2018).

Applying routine activities theory to cybercrime victimization

When RAT was first developed by Cohen and Felson in 1979, it was intended to explain conventional crimes that took place in real or physical locations (Reyns, 2018). However, as technology developed, criminologists looked at how routine activities theory might be used in cybercrime. Theoretically, RAT can be applied to cybercrime victimization because the components of the theory apply to cyberspace as well.

Routine Activity Theory (RAT) was traditionally established on the premise that crimes happen when three factors are involved, which are: motivated criminals, suitable or appropriate targets, and a dearth or absence of guardians converge in place and time (Reyns, 2018). The above presumptions, however, may not be applied to cybercrime, which often involves long-distance communications and online activity. Crimes may take place asynchronously, and offenders may target victims anywhere in the world (Reyns, 2018). This geographical and temporal gap calls into question RAT's fundamental assumptions, rendering it less effective for describing cybercrime.

In the context of offline criminal activity, the term "place" commonly denotes a limited and physically defined region, such as a street. Within this area, criminals may choose their victims based on the situational attributes peculiar to that location. In the context of street crime, offenders may select victims based on their proximity to a desirable target (Wall, 2007). On the other hand, the Internet functions as a digital space that is not restricted by the geographical and spatial limitations

associated with street crime. The absence of close physical proximity to potential targets is negated in the Internet realm, offering a wide range of criminal prospects for determined perpetrators (Newman & Clarke, 2003)

> To solve the spatial and temporal problems of cyberspace, Reyns (2018) suggested

“the "cyber-lifestyle routine activities theory." According to this version, the convergence of motivated offenders, appropriate or suitable targets, and guardianship happens in a networked environment rather than a physical site, the network is the context in which these components interact. Criminal chances in cyberspace no longer need the actual junction of parties in space, offenders may remotely exploit weaknesses or vulnerability of a victim in cyberspace (Reyns, 2018). According to this hypothesis, a networked ecosystem rather than a specific place is where motivated offenders, appropriate targets, and guardianship congregate (Reyns, 2018). These components meet in the network environment, which acts as their environment (Reyns, 2018). The actual physical interaction of parties is no longer necessary to carryout criminal act, remote exploits are available to criminals (Reyns, 2018). For example, cybercrime, such as identity theft, hacking, and online fraud, often don't require immediate physical contact or real-life connection between the offender and victim (Reyns, 2018).

The translation of basic principles of routine activities theory is difficult when adapting RAT to the online environment (Reyns, 2018). For example, proximity, and exposure to suitable offenders used in traditional environments are modified for use in cyberspace or online environment. Converting traditional concepts into online variables has proved difficult and sometimes ineffective or irrelevant (Reyns, 2018). Various studies have included online behavior such as social networking and

dangerous acts as risk factors. In the context of RAT, however, there is variability in how these parameters are operationalized and assessed (Reyns, 2018).

Online Behavioral Risk Factors for Cybercrime Victimization

Studies of cybercrime victimization often investigate the correlations between individuals' online activities, both deviant and routine, and their vulnerability to cybercrimes. The concept of Internet usage frequency has been examined across multiple contexts, with researchers measuring the number of hours individuals spend online on a weekly basis. Holt and Bossler (2013) observed a lack of statistically significant predictive association between Internet usage and victimization by malware infection. Conversely, alternative investigations (e.g., Bergmann et al., 2018) have indicated that heightened frequency of Internet usage is linked to an elevated susceptibility to malware infection, ransomware infection, and the unauthorized exploitation of personal data.

More important than simply examining whether overall Internet usage is related to cybercrime victimization, scholars (see Holt and Bossler, 2016 for a more comprehensive review of online behaviors and cybercrime victimization in general) have examined whether specific online behaviors are related to cybercrime victimization. Online platforms for social networking have evolved into an important platform for the sharing of personal information, frequently without individuals fully understanding the potential risks that may be linked to such actions. The data may comprise personal information such as names, dates of birth, pet names, and phone numbers, which might be exploited for identity theft. Popular social networking networks such as Facebook, Twitter, and LinkedIn have become essential components of individuals' lives, rendering them susceptible to identity theft. In addition, social media has been utilized for fraudulent activities, such as phishing,

wherein criminals impersonate reliable entities in electronic correspondence. The confidence that users have in their social networks and the convenience of accessing a worldwide audience make social media an appealing platform for criminals to perpetrate their fraudulent activities.

According to the Federal Trade Commission (2021), the risk of identity theft is heightened when users disclose an excessive amount of personal information on social media platforms. Specifically, individuals who divulge personal details such as complete names, addresses, phone numbers, and birthdates become more vulnerable to fraudulent activities facilitated by criminals. Van Wilsem (2013) also discovered that online consumer fraud increases with time spent on online shopping and forums. Another study found that Internet scams are linked to online purchases and opening emails from unknown sources (Chen, Beaudoin, & Hong, 2017). The more people reveal their credit or debit card number and the more they disseminate their personal information, the greater the likelihood that they will become victims of cybercrime (Ngo & Paternoster, 2011). Mesch and Dodel (2018) discovered that persons who released personal information online were more likely to receive scam emails. These studies highlight the importance of identifying and addressing potential risks associated with online activities.

Reyns and Henson (2016) used data from the 23rd cycle of the General Social Survey (GSS) performed in Canada in 2009. This is a nationally representative sample of households from all 10 provinces in Canada. Respondents aged 15 and up took part in computer-assisted telephone interviews, yielding a final analytical sample of 11,192 individuals. The chance of online identity theft was positively associated to two online behaviors: online banking and online purchases (Reyns & Henson, 2016).

These behaviors raised the likelihood of victimization by 12% and 17%, respectively (Reyns & Henson, 2016). Booking/reservations and social networking, on the other hand, were not substantially connected to victimization (Reyns & Henson, 2016).

Risky or deviant online behaviors have been found to be related to identity theft victimization as well. Individuals who had encountered hacking were more than twice as likely to have suffered identity theft, and those who had experienced phishing were nearly 40% more likely to have had identity theft (Reyns & Henson, 2016). Individuals whose personal information was made public online were more than three times more likely to be victims of identity theft (Reyns & Henson, 2016). Johnson's (2008) research emphasizes the psychological elements that contribute to the victimization of identity theft. Individuals with high levels of impulsivity and sensation-seeking tendencies are more vulnerable to identity thieves, as they tend to participate in dangerous online behaviors. In addition, engaging in risky behaviors such as visiting websites that are not particularly well-known may enhance the likelihood of being a victim of identity theft committed online (Hille, Walsh, & Cleveland, 2015).

Online Guardianship Protective Factors for Identity Theft Victimization

In addition to examining the relationship between online routine behaviors and cybercrime victimization, scholars also often examine how protective actions decrease the risk of cybercrime victimization. Interestingly, studies do not show consistent findings. To safeguard personal information and reduce the risk of identity theft, the National Cyber Security Centre stresses the significance of maintaining security on public networks. It advises users to use virtual private networks (VPNs) and refrain from accessing sensitive information on public networks (National Cyber Security

Centre, 2021). However, Reyns and Henson's (2016) did not find that any of the online self-protection methods, such as installing antivirus software, deleting emails, or changing passwords, were statistically significant in predicting identity theft in their nationally representative sample of Canadian households.

Although identity theft is frequently categorized as a cybercrime, Ylang (2020) pointed out that the criminals could employ surprisingly easy techniques, such as searching through trash for personal documents (Newman, 2008; Copes and Vieraitis, 2009). This simplicity also shows that reducing one's susceptibility to identity theft may be accomplished by relatively simple self-protective measures.

Demographic Risk Factors for Identity Theft victimization

Sex: According to Harrell (2021), the 2018 Identity Theft Supplement of the National Crime Victimization Survey found that there was there was no significant difference between males and females experiencing identity theft victimization. Both male and female respondents were victimized at the same rate, about 9% for U.S. residents aged 16 or older.

This suggests that gender may not be differentiating in predicting the risk of identity theft.

Some studies, however, find that females are more likely to be victims of identity theft than males (e.g., Johnson & Smith, 2018; Smith and Johnson, 2017). Smith and Johnson's (2017) study revealed that women may be more susceptible to identity theft due to variations in online conduct and gender norms. They also found that women may be more susceptible to social engineering techniques, such as phishing schemes, used by identity thieves (Smith & Johnson, 2017). Martinez et al.

(2019) explored the correlation between gender and identity theft among college students, finding that females are more engaged on social media and more prone to sharing personal information online. Socioeconomic factors, such as lower income levels and the gender pay gap, also contribute to the association between sex and identity theft victimization. These characteristics may worsen the gender disparities in rates of identity theft victimization, hence increasing the appeal of women as targets for identity thieves (Smith, 2017).

Other studies, however, have found that males are more likely to be victims of identity theft than females. According to Johnson et al. (2015), men are more prone to disclosing personal information on social networking platforms, which increases their susceptibility to identity theft. According to Brown's (2018) research, men have a higher susceptibility to phishing scams, which leads to the unauthorized acquisition of personal data. Gendered online behaviors, such as actions taken to safeguard privacy and societal norms, can also play a role in the varying risk of being a victim of identity theft. According to

Williams (2016), females exhibit a higher propensity for participating in these behaviors (Williams, 2016). Davis et al. (2019) also proposed that women tend to exercise greater caution when disclosing personal information over the Internet (Davis et al., 2019).

Race and Ethnicity: According to the 2018 Identity Theft Supplement (Harrell, 2021),

White individuals comprised the largest group of identity theft victims at 10.1%, followed by Hispanics (7.8%), and African-Americans (6.8%). Asians and other racial/ethnic groups experienced victimization at approximately 5.1% and 2.6%, respectively (Harrell, 2021). Although Whites may comprise the largest percentage of

identity theft victims, racial and ethnic minority groups have greater odds of being identity theft victims based on the United
States' racial composition (Harrell, 2021). According to Reyns and Henson's (2016) examination of the Canadian General Social Survey (GSS), non-Whites were 46% more likely to be victimized. These findings suggest that there may be differences in identity theft victimization based on social disparities.

Smith (2015) argues that African Americans and Hispanics exhibit a higher propensity for encountering identity theft in comparison to White counterparts, which can be ascribed to variables including socioeconomic disparities, systematic prejudice, and cultural discrepancies in awareness and preventative efforts. Reynolds (2021) examination of the 2016 National Crime Victimization survey also found that having Hispanic or Latinx ethnicity were important predictors of enduring out-of-pocket losses because of identity theft (Reynolds, 2021).

Gomez (2012) emphasizes the crucial significance of socioeconomic status and its relationship with minority communities in the occurrence of identity theft. Specifically, lowincome persons, who are frequently overrepresented within minority groups, face a dearth of tools and safeguards to counteract theft (Gomez, 2012). The scarcity of resources experienced by these individuals renders them vulnerable to identity thieves, hence emphasizing the necessity for efficient measures to counteract identity theft. Immigrants and ethnic minorities, due to potential language issues, lack of faith in institutions, and unfamiliarity with local laws, may possess less knowledge regarding ways to avoid identity theft, rendering them more vulnerable to theft (Johnson, 2016; Kwan, 2019). These variables can impede individuals' comprehension of the hazards linked to sharing personal information and their ability

to identify possible identity theft, thereby impacting their capacity to report such events (Dixon & Agarwal, 2018).

Household Income: According to the 2018 Identity Theft Supplement, those with higher household incomes have a greater tendency to have been identity theft victims (Harrell, 2021). Households with incomes at or above $75,000 had victimization rates of approximately 12.2%. Households making less than $24,999 had a lower rate of victimization at 6.0% (Harrell, D. 2021). Reyns and Henson's (2016) examination of the Canadian General Social Survey (GSS) found that higher incomes were 11% more likely to victims of identity theft victimization. These findings suggest that households with higher income may be more vulnerable to identity theft victimization.

Identity thieves or criminals are frequently more interested in targeting individuals with higher salaries because they regard them as being wealthier and having greater potential for financial benefit. According to a study conducted by Reilly and Marciniak (2007), those with higher salaries had a greater likelihood of being victims of identity theft in comparison to those with lower incomes (Reilly & Marciniak, 2007) This phenomenon might be attributed to the individuals with higher incomes doing more online shopping, thus potentially increasing more opportunities for identity theft victimization.

Individuals with lower incomes, however, may be more at risk. Identity theft is an alarming problem that impacts or affects individuals of all economic levels, with lowerincome households sometimes being unable to afford to invest in thorough or comprehensive protection measures (Copes, 2016). This may lead to lower-income households being unable to invest in comprehensive security measures (Copes, 2016). Higher income households, on the other hand, may afford to employ credit

monitoring services and buy advanced security systems, which lessens their vulnerability to identity theft (Copes, 2016; Copes, Vieraitis, & Janssen, 2015). In fact, according to a 2019 Federal Trade Commission survey, victims of identity theft reported being most common among people whose family income was less than $25,000, and least common among those whose household income was more than $100,000 (Federal Trade Commission, 2019). People with a low socioeconomic status or those experiencing economic hardship may be more prone to participate in dangerous behaviors, such as divulging personal information in return for money or free gifts (Gross & Acquisti, 2005). Furthermore, people who are under financial stress could be more vulnerable to phishing emails that purport to offer employment or financial assistance, which could cause them to inadvertently divulge sensitive information (Liu & Camp, 2019).

Studies of the 2016 National Crime Victimization Identity Theft Supplement also found that financial losses rose with lower income (Golladay, Holtfreter, & Reynolds, 2021). The findings of this research raise questions about the widely held belief that higher-income people are more vulnerable to identity theft. Instead, data demonstrates that lower-income persons have a greater financial effect and are more likely to suffer personal financial losses because of identity theft (Reynolds, 2021). In addition, the effects of identity theft may have more serious impacts, both emotionally and financially, on lower incomes households as it may be more difficult for them to afford legal assistance, credit repair services, and other necessities (Federal Trade Commission, 2021). This emphasizes the significance of taking the financial effects of identity theft into account and adapting victim care and education to various demographic groups (Reynolds, 2021).

Age: According to the 2018 Identity Theft Supplement (Harrell, 2021), individuals between the ages of 35-49 had the highest rate of victimization (11.0%), making up 29.2% of all victims, while aged 18–24 had the lowest rate of victimization (5.9%). This trend implies that individuals in their prime working and financial years are more appealing targets for identity thieves.

Scholars and government reports, however, demonstrate concern for the elderly regarding identity theft victimization. For example, the Federal Trade Commission (2021) states that elderly people are frequently targeted because of their poor technological knowledge and possible cognitive impairment. Scammers often take advantage of senior citizens by impersonating family members, financial institutions, or governmental organizations, among other strategies. According to the Federal Trade Commission (2021), due to their propensity to divulge personal information, this population group is a prime target for identity theft. Financial literacy is an additional essential component. Older people may be particularly vulnerable to fraudulent schemes or coupons because of their low comprehension of financial institutions and emerging patterns. Individuals may become victims of deceptive investment schemes or disclose personal information in response to phishing efforts (Federal Trade Commission, 2021).

The impact of identity theft on older people is significantly influenced by demographic characteristics, including gender and race. According to research by DeLiema,

Burnes, and Langton (2021), older Black victims of identity theft were more likely than older White victims to have had larger sums of money stolen and to have been affected by the experience.

To contribute to the knowledge on the relationship between online routine activities, online guardianship, and demographics with identity theft victimization using a routine activities framework, this study examines data from a nationally reflective sample, measures key components of routine activities theory, and ran descriptive statistics, correlation analyses, and logistic regression models. It is hypothesized that:

- H1: Increases in online routine behaviors will be related to higher levels of identity theft victimization.
    - H1a: Browsing the Internet more frequently will be related to higher levels of identity theft victimization.
    - H1b: Using social media more frequently will be related to higher levels of identity theft victimization.
    - H1c: Purchasing items online more frequently will be related with higher levels of identity theft victimization.
    - H1d: Storing digital information in cloud-based platforms more frequently will be related with higher levels identity theft victimization.
    - H1e: Using cryptocurrency more frequently will be related with higher levels of identity theft victimization.
    - H1f: Surfing the dark web more frequently will be related with higher levels of identity theft victimization.
- H2: Higher levels of online guardianship will be related to lower levels of identity theft victimization.
    - H2a: Overall online guardianship actions will be related with lower levels of identity theft victimization.

- H2b: Higher levels of computer skills will be related with lower levels of identity theft victimization.

- H3: Demographics will not be significantly related to levels of identity theft victimization.
  - H3a: Sex will not be significantly related with levels of identity theft victimization.
  - H3b: Race and ethnicity will not be significantly related to levels of identity theft victimization.
  - H3c: Age will not be significantly related to levels of identity theft victimization.
  - H3d: Education will not be significantly related to levels of identity theft victimization. ○ H3e: Income will not be significantly related to the levels of identity theft victimization.

CHAPTER 4

METHODOLOGY

Sample Collection

The primary methodological goal was to develop and conduct a survey targeting adult Internet users in the United States who were at least 18 years of age in order to examine the relationship between online routine behaviors, online capable guardianship, demographics, and identity theft victimization. Dr. Cassandra Dodge, Assistant Professor in the Department of Criminal Justice and Criminology at Georgia Southern University, allowed myself and Dr. Adam Bossler to add survey questions to a data collection project that she was about to begin via Qualtrics. The project was approved by the university's Institutional Board Review as H24013.

The survey was conducted in Fall 2023 for a duration of one month. Two sample criteria were used by Qualtrics in the creation of the sample: (1) general population
(nationally reflective); and (2) users must use the Internet. In addition, individuals under the age of 18 were deemed ineligible to take part in the study. Respondents were allowed to take the survey only one time and had 15 minutes to take the survey. Although not a nationally *representative* sample, Qualtrics uses the demographics of respondents to create samples that are nationally *reflective.*

The procedure included the distribution of an online permission form to the participants, which gave them the opportunity to either provide their assent or decline to take part in the study. The user provided consent by selecting "yes" and Qualtrics noted the date. The dates of the respondents who consented were logged by Qualtrics

while their identity was protected, which included the anonymity of their IP handles. It should also be noted that although participants were not compensated directly by the researchers; Qualtrics used incentives to motivate participants to ensure an increase in response rates.

Dr. Dodge's final data collection entailed 917 observations. Roughly ninety percent (91%) of respondents had one or 0 missing responses. See Analytical Plan below for discussion on how missing data were treated.

Measures

Dependent variable: Identity theft victimization

Respondents were asked the same identity theft victimization questions as found in the 2018 National Crime Victimization Survey Identity Theft survey to be able to compare results. The National Crime Victimization survey, as well as the Identity Theft Supplement, asks respondents how often they were victimized over the past 12 months (Harrell, 2021).

This approach attempts to reduce memory recall issues (Maxfield & Babbie, 2018). Respondents frequently have problems accurately recalling information. Cognitive psychologists state that respondents use partial information to attempt to construct responses to surveys (Bradburn, Rips, & Shevell, 1987). These issues may affect the validity of the findings if respondents did not accurately recall that they were victimized or thought that the victimization occurred within the past 12 months and they actually had not.

Checking or savings account identity theft victimization: Respondents were first asked whether they had at least one active checking or savings account through a

bank or financial institution. Respondents who had a checking or savings account were asked whether someone without their permission had used or attempted to use their existing checking or savings account, including any debit or ATM cards, during the past 12 months (0 = no; 1 = yes).

Credit card identity theft victimization: Respondents were also asked whether they have at least one credit card in their name. They were informed to include major credit cards such as a Mastercard or Visa, and store credit cards. They were asked not to include debit cards since that would be related to checking or savings account identity theft victimization. Respondents were then asked whether someone had used or attempted to use one or more of their existing credit cards with their permission (0 = no; 1 = yes).

Other account misuse identity theft victimization: Respondents were asked whether over the past 12 months someone had misused or attempted to misuse another type of existing account such as their telephone, cable, gas, or electric accounts, online payment account like Paypal, insurance policies, entertainment accounts like iTunes, or something else (0 = no; 1 = yes).

New account identity theft victimization: Respondents were asked whether over the past 12 months someone without their permission had used or attempted to use their personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else (0 = no; yes = 1).

Other fraudulent identity theft victimization: Finally, respondents were asked whether over the past 12 months someone used or attempted to use their personal information for some other fraudulent purpose, such as filling out a fraudulent tax

return, getting medical care, applying for a job or government benefits, giving their information to the police when they were charged with a crime or traffic violation, or something else (0 =no; 1 = yes).

Any identity theft victimization: A dichotomous measure was created based on whether the respondent responded yes to any of the five distinct identity theft victimization measures listed above (0 = no; 1 = yes).

Independent variables:

Online Routine Behaviors: Respondents were asked, "To the best of your knowledge, during the previous 12 months, how frequently have you done the following," for the following six items: browsed the Internet; used social media; purchased items online; stored digital information on a cloud-based platform (e.g., Dropbox, Onedrive, Box, iCloud); used cryptocurrency (e.g., Bitcoin); and surfed on the Darkweb. Each item was measured ordinally with four options: never, rarely, sometimes, and often. A reliable scale could not be created (a = 0.577). Therefore, each online routine behavior, consistent with the literature, was kept as a separate measure for the analyses.

Capable guardianship: Respondents were asked seven items (0 = no; 1 = yes) about the following actions during the past 12 months: (1) checked your credit report; (2) changed passwords on any of your financial accounts; (3) purchased identity theft protection from a company that offers protection services; (4) had credit monitoring or identity theft insurance; (5) shredded or destroyed documents containing your personal information?; (6) checked your banking or credit card statements for unfamiliar charges; and (7) used security software program on your computer to

protect against loss of credit cards/card theft (Dodge, 2021). The seven items were added together to create a *capable guardianship* scale ranging from 0 – 7. Chronbach's alpha reliability of the scale was 0.729.

Computer skills: Nine items based on respondent's self-reporting computer knowledge were included in the survey. The options included: very low, below average, average, above average, and very high. The nine items are: dealing with software problems; removing malware from your computer devices (e.g.,, computer viruses); dealing with computer hardware problems identifying if your computer is infected with malware; modifying the firewall on your computing devices; establishing a virtual private network (VPN) on your computing devices; identifying a phishing email (a fake email from unknown sender); identifying misleading or false information online using validated sources; securing digital information (files, documents) through encryption; and surfing the web through anonymous browsers (e.g., TOR). The nine items were averaged to create a *computer skills* scale. The scale had a reliable Chronbach alpha of 0.936.

Controls:

Seven control measures were explored in the following analyses: *age, African-American, other race, Hispanic, age, education,* and *income.*

Sex: The sex of the respondent was measured as a nominal measure in the survey with the categories of: male, female, non-binary, and declined to answer. No respondents declined to answer. Fifteen respondents who reported as non-binary were excluded from the analyses.

The final *sex* measure was coded as: female (0) and male (1).

Race: The race of the respondent was a nominal measure in the survey with the following categories: White, Black or African American, American Indian or Alaska Native, Asian, Native Hawaiian or Pacific Islander, and other. For these analyses, two different race measures were created. *African-American* (1 = yes) are those individuals who identified themselves as Black or African-American according to the survey item. Individuals who identified as American Indian or Alaska Native, Asian, Native Hawaiian or Pacific Islander, or other were categorized as *other race* (1 = yes). *White* (1 = yes) is the comparison group for the analyses.

Hispanic was measured as a nominal measure in the survey with the following categories: Spanish, Hispanic, or Latino (1) (collapsed into category), and not Spanish, Hispanic, or Latino (0). Forty-nine (49) individuals skipped this question and were coded as
0 (not Spanish, Hispanic, or Latino).

Age was measured as a continuous measure.

Highest level of education was measured as an ordinal measure in the survey with eight categories [less than high school degree, high school graduate (high school diploma or equivalent including GED), some college but no degree, Associate degree in college (2-year),
Bachelor's degree in college (4-year), Master's degree, Doctoral degree, and Professional degree (JD, MD). For the analyses, *education* was collapsed into a five category ordinal measure with Master's degree, Doctoral degree, and Professional degree being combined into one final group.

Entire household income was an ordinal measure with eight categories in both the survey and the analyses: less than $10,000; $10,000 to $19,999; $20,000 to $29,999; $30,000 to $39,999; $40,000 to $49,999; $50,000 to $59,999; $60,000 to

$69,999; $70,000 to $79,999; $80,000 to $89,999; $90,000 to $99,999; $100,000 to $149,999; and $150,000 or more.

Analytical Plan:

The initial survey sample consisted of 917 respondents. As a result of missing data, 114 respondents were listwise excluded from the analyses, leaving a final analytical sample of 803 respondents.

In order to examine whether the missing data was significantly different than the analyzed sample, tests of significance were run comparing the two groups. Chi-square tests were run if both measures were dichotomous. Mann-Whitney U tests of significance were run if the independent measure was dichotomous and the dependent measure was categorical. Finally, t-tests were run if one measure was dichotomous and the other measure was continuous. The respondents in the missing data were significantly more likely to be categorized in the *other race* group (missing = 30%; analyzed sample = 18%), be *Hispanic* (missing = 29%; analyzed sample = 16%), be younger (missing = 42.5; analyzed sample = 47), and report lower incomes (missing = 4.85; analyzed sample = 5.7). The two groups were not significantly different, however, regarding whether they had been a victim of identity theft over the past 12 months (using the overall measure) (missing = 35%; analyzed sample = 28%). In addition, the two groups were not significantly different regarding checking/savings identity theft victimization (missing = 23%; analyzed sample = 18%) and credit card identity theft victimization (missing = 10%; analyzed sample = 13%). The two groups, however, were significantly different for the other three categories of identity theft victimization, with the missing data group being more likely to be victims of

other account identity theft victimization (missing = 18%; analyzed sample = 11%), new account identity theft victimization (missing = 14%; analyzed sample = 8%), and other fraudulent purpose identity theft victimization (missing = 13%; analyzed sample = 7%).

Descriptive statistics were run for of all independent and dependent measures included in the study (see Table 1). Descriptive statistics regarding identity theft victimization were compared with statistics from the 2018 Bureau of Justice Statistics Identity Theft Report (Harrell, 2021). Correlation analyses were run between online routine behaviors, online safety precautions, and identity theft victimization (see Table 2). Logistic regression models were run for whether the respondent had been a victim of any form of identity theft victimization over the past 12 months (see Table 3) as well as each specific form of identity theft victimization examined (see Tables 4 – 8).

Results

Twenty-eight percent (28%) of the respondents reported some form of identity theft victimization over the past 12 months (see Table 1). This is over three times as many individuals reported being a victim of identity theft victimization (9%) according to the 2018 Identity Theft Supplement (Harrell, 2021). The most common form of reported identity theft victimization over the past 12 months – 18% -- was whether the respondent had someone used or attempted to use their existing checking or savings account, including any debit or ATM cards, without their permission. Only four percent of respondents reported this type of identity theft victimization in the 2018 Identity Theft Supplement (Harrell, 2021). The next two most common forms of reported identity theft victimization types were whether someone had used

or attempted to use one or more of their existing credit cards without their permission (13%) and whether someone had misused or attempted to misuse another type of existing account, such as telephone or electric accounts, without their permission (11%). According to the 2018 Identity Theft Supplement, only 5% reported being victims of credit card identity theft victimization; less than 1 percent had reported other account identity theft victimization (Harrell, 2021). The least two most common forms of reported identity theft victimization were whether someone had used their personal information to open any new accounts in the respondent's name (8%) or for any other fraudulent purpose (7%). Less than 1% of respondents reported these types of victimization according to the 2018 Identity Theft Supplement (Harrell, 2021). Clearly, respondents reported much higher levels of identity theft victimization in my study.

Table 2 contains the correlations between the online routine behaviors, guardianship, demographics, and identity theft victimization measures. Respondents who spent more time browsing the Internet were not significantly more or less likely to be a victim of identity theft victimization overall, but they were less likely to be victims of four of the five forms of identity theft victimization. Browsing the Internet was not significantly related with credit card identity theft victimization. Using social media more frequently was not significantly related to any of the measures of identity theft victimization. Purchasing items online more frequently was significantly and positively related with both overall identity theft victimization and credit card identity theft victimization. Three online routine behavior measures – storing digital information on cloud-based platforms, using cryptocurrency, and surfing the Darkweb – were positively and significantly related with the overall

identity theft victimization measure as well as each of the five specific forms of identity theft victimization examined. These last findings support the hypotheses that specific online routine behaviors are significantly related with identity theft victimization.

Both measures of guardianship – the total online guardianship scale and reported computer skills – were significantly and positively related with the overall identity theft victimization measure as well as all five specific indicators (see Table 2). These findings are contradictory to the hypotheses which state that guardianship should decrease victimization.

Demographic measures were not strongly correlated with reported identity theft victimization measures (see Table 2). Gender, race, and ethnicity measures were not significantly correlated with any of the dependent measures. Age, however, was negatively correlated with the overall identity theft victimization measure as well as savings account victimization, other account victimization, new account victimization, and other form of fraud victimization. In other words, older respondents were less likely to report these forms of victimization. Higher levels of education and income were only significantly and positively correlated with one form of victimization – credit card fraud victimization.

The overall findings of the correlation analyses strongly supported additional multivariate analyses. With all identity theft victimization measures being dichotomous in nature, logistic regression models were run to examine the odds of the respondents' being victims of identity theft victims, whether overall (see Table 3) or for any of the five specific forms of identity theft victimization explored (see Tables 4 -8). Multicollinearity diagnostics were run for the full logistic regression model. The using cryptocurrency measure had the highest variance inflation factor

(VIF) at 1.607 and the lowest tolerance level (0.622). Thus, the muticollinearity diagnostics indicated that all VIFs and tolerance levels were within acceptable limits.

Table 3 contains the findings of the logistic regression analyses running online routine behaviors, online guardianship, and demographics on the odds of being a victim of any of form of identity theft victimization over the past 12 months. Three online routine behaviors were significantly related to the odds of being a victim of identity theft victimization.

Individuals who browsed the Internet more often were less likely to be victimized [Exp(B) =

0.655]. Individuals who stored digital information on a cloud-based platform [Exp(B) = 1.276] and used cryptocurrency more often [Exp(B) = 1.336] had higher odds of being a victim of identity theft victimization. When examining Tables 4 -8, which contain the logistic regression findings consisting of the specific forms of identity theft victimization, we find that spending more time browsing the Internet specifically decreased the odds of checking/savings account identity theft victimization [Exp(B) = 0.612] (see Table 4), other type of account identity theft victimization [Exp(B) = 0.633] (see Table 6), new account identity theft victimization [Exp(B) = 0.577] (see Table 7), and other fraudulent purpose identity theft victimization [Exp(B) = 0.565] (see Table 8). Purchasing items online more frequently only increased the odds of credit card identity theft victimization [Exp(B) = 1.481] (see Table 5). Although storing digital information in cloud-based platforms significantly increased the odds of being a victim of identity theft victimization, this online behavior was not significantly related with any of the five specific types examined. Using cryptocurrency more frequently specifically increased the odds of

other type of account identity theft victimization [Exp(B) = 1.347] (see Table 6), new account identity theft victimization
[Exp(B) = 1.426] (see Table 7), and other fraudulent purpose identity theft victimization [Exp(B) = 1.635] (see Table 8). Finally, surfing the Darkweb increased the odds of other fraudulent purposes of identity theft victimization [Exp(B) = 1.886] (see Table 8).

Higher scores on the online guardianship scale significantly increased the odds of overall identity theft victimization [Exp(B) = 1.173] (see Table 4), contradictory to the proposed hypotheses. Higher levels of online guardianship significantly increased the odds of both existing credit card identity theft victimization [Exp(B) = 1.337] (see Table 5) and other fraudulent purpose identity theft victimization [Exp(B) = 1.294] (see Table 8). Reporting higher levels of computer skills was not significantly related with any form of identity theft victimization.

Similar to the correlation analyses, demographics overall were not strongly related with the odds of identity theft victimization when controlling for other measures (see Tables 4 – 8). In fact, no demographic measure was significantly related with the odds of overall identity theft victimization (see Table 4). Only two demographic measures were significantly related with any of the specific forms of identity theft victimization. African Americans were less likely than Whites to report being victims of other fraudulent purpose ID theft victimization [Exp(B) = 0.294] (see Table 8). Older Americans were less likely to be victims of new account ID theft victimization [Exp(B) = 0.962] (see Table 7) and other fraudulent purpose identity theft victimization [Exp(B) = 0.950] (see Table 8).

CHAPTER 5

DISCUSSION AND CONCLUSION

Routine activities theory (RAT) (Cohen and Felson, 1979) provides helpful hypotheses on how online routine behaviors and guardianship may be related to identity theft victimization. Based on the theory and the literature (see Reyns, 2018 for overall summary), it was hypothesized that increases in online routine behaviors will be related with higher levels of identity theft victimization (H1). Specifically, it was hypothesized that higher levels of browsing the Internet (H1a), using social media (H1b), purchasing items online (H1c), storing digital information in cloud-based platforms (H1d), using cryptocurrency (H1e), and surfing the Dark web (H1f) would be significantly related with higher levels of identity theft victimization.

Hypotheses H1a was rejected as spending more time browsing the Internet was related with *lower* levels of identity theft victimization. H1b was also rejected as using social media more frequently was not significantly related with higher levels of any form of identity theft victimization. The other four measures provided more support for RAT as partial support was found in the correlation analyses and/or the logistic regression analyses regarding storing purchasing items online (H1c), storing digital information in cloud-based platforms (H1d), using cryptocurrency (H1e), and surfing the Dark web (H1f). Thus, the majority of the online routine behaviors examined were significantly related to identity theft victimization in the predicted direction.

The significant relationship found in this study between online purchases and identity theft victimization supports the findings of previous studies that found that

online purchases to be related to online fraud, Internet scams, and identity theft victimization (Chen et al.

2017; Reyns & Henson, 2016; Van Wilsem, 2013). My study supported Reyns and Henson's (2016) finding that social networking (i.e. social media) was not related with identity theft victimization. Most previous studies (e.g., Reyns and Henson, 2016) included risky online behaviors, such as sharing personal information. In this study, I did not have measures that were similar to previous studies regarding risky online behaviors. However, this study was unique in that it contained survey items that other studies did not have, such as storing digital information, using cryptocurrency, and surfing the Dark web. The partial support that was found in this study for the relationship between storing digital information in a cloud-based platform, using cryptocurrency, and surfing the Dark web indicates that there are other risky behaviors that routine activities scholars need to start examining.

Based on RAT, it was hypothesized that higher levels of overall guardianship (H2a) and computer skills (H2b) would be related with lower levels of identity theft victimization. Both of these hypotheses were rejected, but for different reasons. H2a was rejected because higher levels of online guardianship was significantly and *positively* related with *higher* levels of identity theft victimization in both the correlation analyses and logistic regression models. H2b was rejected because higher levels of computer skills were related with *higher* levels of identity theft victimization in the correlation analyses. Higher computer skills were not significantly related with identity theft victimization in the fuller logistic regression models. Although this study's findings reject the hypotheses, the findings are similar to that of previous studies that found a positive relationship (see Holt and Bossler, 2016). However, other studies, such as Reyns and Henson (2016), did not find that

online capable guardianship, such as installing antivirus software, deleting emails, or changing passwords, was significantly related with identity theft victimization in Canada.

Holt and Bossler's (2016) summary of cybercrime research may provide some suggestions on why online guardianship may be positively related with identity theft victimization. First, one of the limitations of this study was that cross-sectional data was used. Most measures, including the dependent measures, asked respondents about the past 12 months. Therefore, the dependent measures are capturing data over the same time period as the independent measures. Instead of overall online guardianship leading to higher levels of identity theft victimization, it is as probable that identity theft victimization may increase the guardianship measures that respondents may take. For the most part, only longitudinal data can address this issue. Second, it is also possible that online guardianship is positively related with identity theft victimization because individuals who check their credit scores, who keep track of online purchases, etc. are more aware than those who do not that they were victims of identity theft victimization.

Finally, previous literature was inconsistent regarding the relationship between most demographics and identity theft victimization (e.g., Harrell, 2021; Reilly and Marciniak, 2007). Therefore, it was hypothesized that no demographic measure would be significantly related with identity theft victimization (H3a - e). Overall, the findings of this study support the null hypotheses. Sex (H3a), race and ethnicity (H3b) were not significantly related with identity theft victimization in either the correlation analyses or the logistic regression models. The only exception is that African-Americans were less likely than Whites to be victims of other fraud

identity theft victimization. The relationship between age and identity theft victimization had the strongest support of any of the demographic measures (H3c). The correlation analyses indicate that older Americans are less likely to be victims of identity theft victimization. In addition, in the full logistic regression models, older Americans were still less likely to be victims of new account identity theft victimization and other fraud identity theft victimization. This finding is consistent with that of the Federal Trade Commission's (2021) argument that the elderly are targeted, potentially because of lower technological knowledge. According to this report, this population may be more likely to divulge personal information on social media or to scammers. Therefore, the negative relationship between age and identity theft victimization may be a result of our study not controlling for the risky sharing of personal information. It may also indicate that the computer skills measure does not truly capture differences in computer skills across age groups. Education (H3d) and income (H3e) were both positively, but weakly correlated with credit card identity theft victimization. Neither measure, however, was significantly related with any form of identity theft victimization in any of the logistic regression models.

As with any study, this thesis has limitations as well. As previously stated, the dataset used consisted of cross-sectional data. This limitation is quite common in the routine activities and identity theft victimization literature (Golladay, 2017; Golladay & Holtfreter, 2017; Reyns & Henson, 2016; Ylang, 2020)). This prevents assessing proper temporal ordering. In other words, it is not possible to know whether the independent measures actually occurred in time before the dependent measures. Therefore, the study is examining correlation and not causation. Kemp and Perez

(2023) also states that this leads to difficulties in evaluating cybercrime prevention measures using cross-sectional data. Future researchers may address this issue with the creation of longitudinal data sets that will allow for the assessment of proper temporal ordering. This is particularly important to assess whether victims alter their online behaviors and online guardianship after victimization.

Next, the dataset consists of a nationally reflective sample. Qualtrics created a dataset that matched the United States on demographics and whether they used the Internet. However, only individuals who are interested in taking online surveys are included in the sample. This may explain the much higher identity theft victimization levels as reported by the respondents. The 2018 Identity Theft Supplement (Harrell, 2021) tried to capture a more nationally representative sample of individuals, some of who do not use the Internet for almost any purposes, such as online banking and shopping. In this sample, the use of the

Internet was one of the two primary characteristics that Qualtrics used to create the sample.

It should also be noted that the Identity Theft Supplement collected its data in 2018 and the sample used for this thesis was collected in the Fall 2023. Increases and changes in both technological uses and identity theft victimization may have occurred over that time. Finally, it should be noted that the informed consent report indicated that the survey was about online behaviors, cybercrime, and victimization. Thus, there may be significant self-selection occurring where individuals who are interested in the topic, possibly because they were victims of identity theft, decided to participate in the survey.

Third, measurement issues can always be a problem. Although this study used the same identity theft victimization measures as the 2018 Identity Theft

Supplement (Harrell, 2021), it still leads to the problem of inaccurate recall when respondents are self-reporting victimization (Golladay, 2017; Golladay & Holtfreter, 2017). The study also did not include measures on traditional "risky" online routine behaviors, such as sharing personal information online or pirating media (Reyns and Henson, 2016). In addition, the measure on browsing the Internet is quite broad and does not ask respondents about specific types of websites that they visit. Similarly, the analyses in this study only examined the frequency of social media usage, but did not go into any depth on the specific social media websites/apps that respondents use. That said, the study found interesting results regarding the use of cryptocurrency and surfing the Dark web. It is therefore recommended that future studies go into more depth on survey questions regarding the websites that respondents visit, as well as the type of social media they most often use. In addition, it is recommended that scholars start considering including measures on the use of cryptocurrency and the Dark web in their studies on identity theft victimization specifically and cybercrime victimization generally. It should also be noted that in this study, I examined overall identity theft victimization and five specific forms in the analyses. However, the analyses assumed that the risk predictors were the same for all demographic groups. Previous research (e.g., Parti, 2023) found evidence that the factors for online fraud victimization differed by age. Other scholars found that older Americans may be more likely and may have different financial and emotional responses to being victims of identity theft victimization (Kemp & Perez,

2003). Kemp and Perez (2003)'s analysis of the Ipsos' 2019 survey on "Scams and Fraud

Experienced by Consumers" on behalf of the European Commission supported the need for targeted interventions that consider both financial and non-financial

consequences, and improving responses to fraud cases. Their study also highlight the changing landscape of online fraud and older people's Internet habits, emphasizing the importance of ongoing research in this area. Interventions for fraud victims who are adults or older should emphasize not only their financial recovery but also their general well-being and social connections (Kemp & Erades Pérez, 2023). Support services should include psychological counseling to assist older consumers in dealing with the emotional consequences of fraud. Policymakers and institutions must improve their responses to fraud, as victims frequently express dissatisfaction with the assistance they receive.

Supporting the arguments of previous scholars (e.g., Holt and Bossler, 2016; Parti, 2023; Reyns, 2018), the findings of this study support examining the predictors of specific forms of cybercrime rather than cybercrime as a general category. In fact, in this study, it was found that the predictors of identity theft victimization differed depending on the specific form being analyzed. By educating people about how common specific scams are, and how they may lead to specific forms of identity theft victimization, potential victims may actually be less likely to become actual victims. Taking preventative online guardianship measures:

Ylang's (2020) examination of the 2014 Identity Theft Supplement indicates that self-defense measures do not have to be technologically complicated or expensive. Basic precautions such as eliminating personal papers and monitoring or keeping tabs bank accounts can be quite effective. According to the report, authorities must concentrate on proactive measures for prevention and awareness, beginning with financial literacy instruction in schools. A proactive strategy to preventing identity theft by policymakers might be beneficial, this approach should emphasize public

education, awareness-raising, and useful guidance, particularly in schools where it can foster financial literacy and information protection.

Supporting previous research (e.g., Golladay and Holtfreter, 2017; Reyns and Henson, 2016), integrating criminological theory into education awareness programs and victim assistance programs is necessary. Policymakers and Internet service providers should think of fresh approaches to stop identity theft, maybe including environmental criminology concepts (Reyns & Henson, 2016). In addition, victims can be encouraged to report crimes and ask for help, which will ultimately make them less susceptible to scams in the future
(Parti, 2023).

Although this study did not examine the police response to identity theft victimization, it is almost impossible to not state the importance of improving citizen reporting of identity theft victimization to the police and their response to it (Cross and Blackshaw, 2014). In addition to causing victims to suffer severe financial losses and psychological distress, online fraud is often underreported (Cross & Blackshaw, 2014). Cross and Blackshaw's (2014) report emphasize the difficulties law enforcement organizations have when looking into Internet fraud, especially since it is virtual and international in nature. They argued for the need of a proactive strategy in the fight against online fraud, using financial intelligence to find victims who may not be aware of or disclose their abuse. This strategy dramatically lessens the suffering and financial losses that victims go through. Additionally, it encourages cooperation between law enforcement authorities and helps to legitimize the experiences of victims.

Identity theft victimization is a growing exponential problem for American citizens as evidenced by government reports (e.g., Harrell, 2021) and scholarly

research (e.g., Golladay, 2017). Scholars have attempted to use routine activities theory (Cohen and Felson, 1979) as a framework to understand how online routine activities, online guardianship, and demographics are related with identity theft victimization (e.g., Reyns and Henson, 2016). The findings of this study provided partial support for previous research as it found that certain online behaviors, such as purchasing items online, using cryptocurrency, and surfing the Dark web, are related with higher levels of identity theft victimization. Higher levels of online guardianship, however, were related with higher levels of identity theft victimization, not lower. The findings support continued use of routine activities theory as a useful framework to understand cybercrime victimization. In addition, the findings may suggest that policies and education campaigns should be tailored toward specific forms of identity theft victimization. The victimization of cybercrime is a notable concern, especially for susceptible demographics such as the elderly and individuals with low proficiency or knowledge in digital technology. Policymakers should contemplate adopting steps to bolster these susceptible communities and allocate resources for victims of cybercrime. One such approach is to improve digital literacy and cybersecurity education initiatives. Implementing specialized assistance programs and helplines for victims, partnering with local community groups to detect and assist persons who have been victimized, and campaigning for more robust laws and regulations to safeguard consumers. In addition Considering the distinct difficulties and consequences associated with identity theft, authorities should contemplate the adoption of focused regulations and measures to tackle this particular kind of cybercrime victimization. These measures may involve improving credit monitoring and fraud alert systems, simplifying the procedure for victims to report

identity theft, and providing easier access to support services Imposing tougher security standards and data protection regulations on companies and organizations Increasing funds and resources for law enforcement agencies to investigate and prosecute identity theft cases, as well as investigating the viability of establishing a national identity theft register or database to track and monitor instances and aid victims. The internet's lack of geographical boundaries been a networked environment and its operational simplicity across different jurisdictions provide substantial obstacles for law enforcement, international accords and treaties can help develop uniform legal frameworks and expedite suspect extradition.

REFERENCES

Allison, S. F. H., Schuck, A. M., & Lersch, K. M. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33* (1), 19 – 29.

Bergmann, M. C., Dreißigacker, A., von Skarczinski, B., & Wollinger, G. R. (2018). Cyberdependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking, 21*(2), 84–90. DOI:10.1089/cyber.2016.0727

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 974 – 2891.

Bradburn, N.M., Rips, L.J., & Shevell, S.K. (1987). Answering autobiographical questions: The impact of memory and inference on surveys. *Science, 236* (4798), 157-161. DOI: 10.1126/science.3563494

Brooks, T. (2003). *Security awareness: Applying practical security in your world.* 5th edition. Pearson Education. Bureau of Justice Statistics (n.d.). *About BJS.* Last accessed on 4/02/2024 at https://bjs.ojp.gov/about.

Bureau of Justice Statistics (n.d.). *Identity Theft and Financial Fraud.* Last accessed on

Bureau of Justice Statistics (n.d.). *Identity Theft Supplement (ITS).* Last accessed on

4/02/2024 at https://bjs.ojp.gov/data-collection/identity-theft-supplement-its#surveys-0 4/02/2024 at https://bjs.ojp.gov/topics/crime/identity-theft

Bureau of Justice Statistics (n.d.). *National Crime Victimization Survey (NCVS)*. Last accessed on 4/02/2024 at https://bjs.ojp.gov/data-collection/ncvs#methodology-0

Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*, 101058. https://doi.org/10.1016/j.pmedr.2020.101058

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104. https://doi.org/10.1080/10864415.2004.11044320

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. DOI:10.2307/2094589

Copes, H. (2016). Sensitive spaces: Identity theft and victimization. *British Journal of Criminology, 56*(4), 661-678. doi:10.1093/bjc/azv119

Copes, H., & Vieraitis, L. M. (2009). Bounded rationality of identity thieves: Using offenderbased research to inform policy. *Criminology and Public Policy, 8*(2), 237-262. https://doi.org/10.1111/j.1745-9133.2009.00553.x

Cross, C., & Blackshaw, D. (2014). Improving the Police Response to Online Fraud.*Policing, 9*(2), 119–128. DOI:10.1093/police/pau044

Dixon, B., & Agarwal, N. (2018). Racial and ethnic differences in identity theft victimization and monetization: Evidence from panel data. *Journal of Consumer Affairs, 52*(1), 202-231.

Dodge, C. (2021). *The ring of Gyges 2.0: How anonymity providing behaviors affect willingness to participate in online deviance* (Publication No. 28548152) [Doctoral dissertation, University of South Florida]. ProQuest Dissertations Publishing. Federal

Trade Commission. (1998). *Identity Theft and Assumption Deterrence Act*. Washington, DC: Federal Trade Commission. https://www.ftc.gov/node/119459

Federal Trade Commission. (2019). *Identity theft: What to know, what to do*. Retrieved from https://www.consumer.ftc.gov/topics/identity-theft

Federal Trade Commission. (2019). *Consumer Sentinel Network Data Book 2019*. Retrieved From https://www.ftc.gov/system/files/documents/reports/consumer-sentinelnetwork-data-book-2019/consumer_sentinel_network_data_book_2019.pdf.

Federal Trade Commission. (2021). *Identity Theft.* Retrieved from https://www.consumer.ftc.gov/features/feature-0014-identity-thef.

Federal Trade Commission. (2022, February). Consumer Sentinel Network Data Book 2021.

Retrieved from https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%20

2021%20Final%20PDF.pdf.

Federal Trade Commission. (2022). Consumer Sentinel Network Data Book 2021.

https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021

Fruhlinger, J. (2020, February 12). The OPM hack explained: Bad security practices met

China's Captain America. CSO. Available at:

https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-

securitypractices-meet-chinas-captain-america.html

Golladay, K. A. (2017). Reporting behaviors of identity theft victims: an empirical test of

Black's theory of law. *Journal of Financial Crime, 24*(1), 101-117. doi:10.1108/JFC-

01-2016-0010

Golladay, K., & Holtfreter, K. (2017). The Consequences of Identity Theft Victimization: An

Examination of Emotional and Physical Health Outcomes. Victims & Offenders,

12(5), 741–760. http://dx.doi.org/10.1080/15564886.2016.1177766

Gomez, M. (2012). Identity theft among low-income urban residents: Implications for policy.

Journal of Poverty, 16(3), 356-372.

Harrell, D. (2021, April). Victims of Identity theft. *Bureau of Justice Statistics.*

https://bjs.ojp.gov/content/pub/pdf/vit18.pdf

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of*

technology-enabled offenses. Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and digital*

forensics: An introduction. 3rd edition. Routledge.

Hu, X., Zhang, X., & Lovrich, N. (2021). Forecasting Identity Theft Victims: Analyzing

Characteristics and Preventive Actions through Machine Learning Approaches.

Victims & Offenders, 16(4), 465–494. doi:10.1080/15564886.2020

Internet Crime Complaint Center. (2022). *Internet Crime Report 2021. Federal*

Bureau of Investigation. Retrieved from

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Irshad, S., & Soomro, T. R. (2018). Identity theft and social media. *International Journal of*

Computer Science and Network Security 18(1): 43-55.

Johnson, A. (2016). Understanding the impact of culture on identity theft

victimization and prevention. *Journal of Cultural Diversity, 23*(2), 45-62.

Johnson, A. B., & Smith, C. D. (2018). Gender and identity theft victimization: A

comparison of men and women. *Journal of Financial Crime, 25*(3), 681-694.

Kemp, S., & Erades Pérez, N. (2023). Consumer Fraud against Older Adults in

Digital Society:Examining Victimization and Its Impact. *International*

Journal of

Environmental Research and Public Health, 20, 5404.

https://doi.org/10.3390/ijerph20075404

Kshetri, N. (2010). *The global cybercrime industry: Economic, institutional and*

strategic perspectives. 2010th edition. Springer Science & Business Media.

Kwan, M. P. (2019). Ethnic differences in identity theft victimization: A spatial analysis.

Security Journal, 32(3), 282-298.

Martinez, L. R., Thompson, S. J., & Marotta, S. A. (2019). Gender and identity theft victimization among college students. *Journal of Interpersonal Violence, 34*(9), 1925-
1947.

Maxfield, M.G., and Babbie, E.R. (2018). *Research methods for criminal justice and criminology. 8th edition*. Cengage.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist, 62*, 1356–1371

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology, 5*, 773–793

Parti, K. (2023). What is a capable guardian to older fraud victims? Comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory.
Frontiers in Psychology (14).
https://www.frontiersin.org/articles/10.3389/fpsyg.2023.1118741/full

Ramirez, L. (2018). Racial profiling and identity theft: A critical examination. *Journal of*
Ethnicity in Criminal Justice, 16(4), 289-308.

Reilly, P., & Marciniak, M. (2007). Income levels and identity theft: A preliminary analysis of the relationship between income levels and identity theft victimization. *Journal of Financial Crime, 14*(2), 195-204.

Reyns, B. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and*

Delinquency, 50(2), 216-238.

Reyns, B. W. (2018). Routine activity theory and cybercrime: A theoretical appraisal and literature review. In K. F. Steinmetz & M. R. Nobles (Eds.), *Technocrime and Criminological Theory* (pp. 35-54). Routledge.

Reyns, B. W., & Henson, B. (2016). The thief with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10), 1119-1139. doi:10.1177/0306624X15572861

Reynolds, D. (2021). The differential effects of identity theft victimization: how demographics predict suffering out-of-pocket losses. *Security Journal, 34*(4), 737-754. https://doi.org/10.1057/s41284-020-00258-y

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare data breaches: Insights and implications. *Healthcare (Basel), 8(*2), 133. [DOI: 10.3390/healthcare8020133]

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., Hutton, S., 2004. Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Science, 49* (1), 1–6. https://doi.org/10.1520/JFS2003178

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age*. NYU Press.

Smith, J. (2015). Racial disparities in identity theft victimization: An analysis of national data. *Race and Social Problems, 7*(2), 123-138.

Smith, S. (2017). Gender differences in online security behaviors: Examining the moderating effects of age and income. *Journal of Financial Crime, 24*(3), 369-384.

Smith, C. D., & Johnson, A. B. (2017). Phishing victimization and gender: A comparison of men and women. *Journal of Financial Crime, 24*(1), 149-162.

U.S. Department of Justice. (2021). Ide ntity Theft. https://www.justice.gov/criminalfraud/identity-theft/identity-theft-and-identity-fraud U.S Office of Personnel Management (n.d.). Cybersecurity Resource Center. Available at: https://www.opm.gov/cybersecurity-resource-center/#url=Overview

Ylang, N. (2020). Capable guardianship against identity theft: Demographic insights based on a national sample of US adults. Journal of Financial Crime, 27(1), 130-142. DOI: 10.1108/JFC-12-2018-0140.

APPENDIX

Table 1. Descriptive Statistics (N = 803).

	Mean or (%)	SD	Range
Dependent Variable			
Any ID Theft Victimization	0.28	0.45	0-1
Checking/savings ID theft victimization	0.18	0.38	0-1
Existing credit card ID theft victimization	0.13	0.34	0-1
Other account ID theft victimization	0.11	0.31	0-1
New account ID theft victimization	0.08	0.27	0-1
Other purpose ID theft victimization	0.07	0.25	0-1
Online routine behaviors			
Browsed the Internet	2.77	0.54	0-3
Used social media	2.43	0.93	0-3
Purchased items online	2.22	0.82	0-3
Stored digital information on cloud-based platform	1.54	1.15	0-3
Used cryptocurrency	0.46	0.89	0-3
Surfed on the Darkweb	0.25	0.67	0-3
Guardianship			
Total online guardianship	3.65	1.97	0-7
Computer skills	2.61	1.01	1-5
Demographics			
Male	0.50	0.50	0-1
White	0.73	0.44	0-1
Black or African-American	0.13	0.34	0-1
Other race	0.18	0.39	0-1
Hispanic	0.16	0.37	0-1
Age	47.02	18.31	18-96
Education	3.52	1.45	1-6
Income	5.70	3.41	1-12

Table 2: Correlation matrix of measures (N = 803).

	1	2	3	4	5	6
Online routine behaviors						
Browsed the Internet	-0.062	-0.077*	0.026	-0.074*	-0.104*	-0.148*
Used social media	0.020	0.043	0.023	0.020	0.012	-0.025
Purchased items online	0.102*	0.068	0.147*	0.057	0.027	-0.019
Stored digital information	0.171*	0.117*	0.161*	0.081*	0.102*	0.088*
Used cryptocurrency	0.222*	0.159*	0.203*	0.197*	0.245*	0.324*
Surfed on the Darkweb	0.195*	0.174*	0.200*	0.197*	0.244*	0.360*
Guardianship						
Total online guardianship	0.176*	0.111*	0.226*	0.106*	0.100*	0.124*
Computer skills	0.096*	0.075*	0.102*	0.093*	0.104*	0.085*
Demographics						
Male	-0.042	-0.035	-0.015	-0.009	0.021	0.047
Black or African-American	-0.006	0.019	0.015	0.042	-0.006	-0.018
Other race	0.004	-0.021	-0.009	-0.021	0.038	-0.040
Hispanic	0.023	0.003	-0.009	0.008	0.068	0.039
Age	-0.099*	-0.078*	-0.039	-0.096*	-0.197*	-0.197*
Education	0.013	0.017	0.095*	0.007	-0.005	-0.030
Income	0.056	0.017	0.098*	0.054	0.003	-0.002

Notes: 1 = Any ID theft victimization; 2 = Checking or savings account ID theft victimization; 3 = Credit card victimization ID theft victimization; 4 = Other account ID theft victimization; 5 = New account ID theft victimization; 6 = Other purpose ID theft victimization

Significance levels: $p \leq .05$*

Table 3. Logistic Regression Model for: Any ID Theft Victimization (n = 803)

	B	S.E.	Exp(B)	Sig.
Online routine behaviors				
Browsed the Internet	-0.422	0.164	0.655	0.010**
Used social media	-0.066	0.104	0.936	0.528
Purchased items online	0.161	0.123	1.175	0.190
Stored digital information	0.244	0.090	1.276	0.007**
Used cryptocurrency	0.290	0.108	1.336	0.007**
Surfed the Darkweb	0.221	0.141	1.247	0.119
Online Guardianship				
Total online guardianship	0.160	0.048	1.173	<0.001***
Computer skill	-0.008	0.096	0.992	0.934
Demographics				
Male	-0.333	0.197	0.717	0.092
Black/African-American	-0.296	0.273	0.744	0.278
Other race	-0.040	0.234	0.961	0.864
Hispanic	-0.021	0.249	0.979	0.933
Age	-0.005	0.006	0.995	0.388
Education	-0.081	0.068	0.922	0.231
Income	0.006	0.029	1.006	0.831
Constant	-0.499	0.576	0.607	0.386
Chi-square (df)	79.920* (15)			
-2LL	872.665			
Nagelkerke R^2	0.136			

Note: *p<.05, **p<.01, ***p<.001

Table 4. Logistic Regression Model for: Existing Checking/Savings Account ID Theft Victimization (n = 803)

	B	S.E.	Exp(B)	Sig.
Online routine behaviors				
Browsed the Internet	-0.491	0.179	0.612	0.006**
Used social media	0.079	0.126	1.082	0.533
Purchased items online	0.141	0.142	1.151	0.319
Stored digital information	0.176	0.104	1.192	0.091
Used cryptocurrency	0.166	0.121	1.181	0.169
Surfed the Darkweb	0.272	0.149	1.312	0.068
Online Guardianship				
Total online guardianship	0.104	0.055	1.110	0.058
Computer skill	0.024	0.109	1.025	0.824
Demographics				
Male	-0.314	0.277	0.731	0.167
Black/African-American	-0.158	0.303	0.853	0.601
Other race	-0.187	0.277	0.829	0.500
Hispanic	-0.167	0.289	0.847	0.565
Age	-0.004	0.007	0.996	0.496
Education	-0.009	0.077	0.991	0.911
Income	-0.024	0.034	0.977	0.481
Constant	-1.018	0.643	0.361	0.113
Chi-square (df)	44.820 (15)			
-2LL	710.598			
Nagelkerke R^2	0.089			

Note: *p<.05, **p<01, ***p<.001

Table 5. Logistic Regression Model for: Existing Credit Card ID Theft Victimization (n = 803)

	B	S.E.	Exp(B)	Sig.
Online routine behaviors				
Browsed the Internet	-0.133	0.241	0.876	0.583
Used social media	-0.127	0.142	0.881	0.370
Purchased items online	0.393	0.189	1.481	0.037*
Stored digital information	0.217	0.127	1.242	0.087
Used cryptocurrency	0.227	0.136	1.255	0.095
Surfed the Darkweb	0.290	0.166	1.337	0.080
Online Guardianship				
Total online guardianship	0.290	0.069	1.337	<.001***
Computer skill	-0.073	0.129	0.929	0.570
Demographics				
Male	-0.237	0.266	0.789	0.373
Black/African-American	0.089	0.361	1.094	0.804
Other race	0.123	0.323	1.131	0.703
Hispanic	-0.063	0.349	0.939	0.857
Age	-0.001	0.008	0.999	0.884
Education	0.041	0.091	1.042	0.655
Income	0.009	0.040	1.009	0.817
Constant	-3.858	0.878	0.021	<.001***
Chi-square (df)	76.058 (15)			
-2LL	539.173			
Nagelkerke R^2	0.169			

Note: *p<.05, **p<.01, ***p<.001

Table 6. Logistic Regression Model for: Other Type of Account ID Theft Victimization (n = 803)

	B	S.E.	Exp(B)	Sig.
Online routine behaviors				
Browsed the Internet	-0.458	0.213	0.633	0.031*
Used social media	-0.008	0.158	0.992	0.961
Purchased items online	0.176	0.181	1.193	0.331
Stored digital information	0.033	0.132	1.034	0.801
Used cryptocurrency	0.298	0.139	1.347	0.033*
Surfed the Darkweb	0.256	0.165	1.292	0.121
Online Guardianship				
Total online guardianship	0.107	0.068	1.112	0.119
Computer skill	0.106	0.135	1.112	0.431
Demographics				
Male	-0.234	0.284	0.791	0.409
Black/African-American	0.215	0.357	1.240	0.547
Other race	-0.077	0.349	0.926	0.825
Hispanic	-0.068	0.355	0.934	0.848
Age	-0.009	0.008	0.991	0.259
Education	-0.101	0.096	0.904	0.294
Income	0.039	0.041	1.040	0.343
Constant	-1.634	0.780	0.195	0.036*
Chi-square (df)	45.003 (15)			
-2LL	505.916			
Nagelkerke R^2	0.110			

Note: *p<.05, **p<.01, ***p<.001

Table 7. Logistic Regression Model for: New Account ID Theft Victimization (n = 803)

	B	S.E.	Exp(B)	Sig.
Online routine behaviors				
Browsed the Internet	-0.550	0.236	0.577	0.020*
Used social media	-0.105	0.198	0.900	0.595
Purchased items online	0.106	0.214	1.112	0.620
Stored digital information	0.167	0.164	1.182	0.309
Used cryptocurrency	0.355	0.154	1.426	0.021*
Surfed the Darkweb	0.318	0.181	1.375	0.078
Online Guardianship				
Total online guardianship	0.147	0.079	1.158	0.061
Computer skill	0.089	0.156	1.093	0.568
Demographics				
Male	0.261	0.346	1.298	0.451
Black/African-American	-0.367	0.464	0.693	0.429
Other race	0.331	0.370	1.392	0.372
Hispanic	0.282	0.387	1.326	0.467
Age	-0.039	0.011	0.962	<.001***
Education	-0.042	0.116	0.959	0.719
Income	-0.031	0.050	0.970	0.541
Constant	-0.773	0.888	0.461	0.384
Chi-square (df)	78.311 (15)***			
-2LL	368.220			
Nagelkerke R^2	0.218			

Note: *p<.05, **p<.01, ***p<.001

Table 8. Logistic Regression Model for: Other Fraudulent Purpose ID Theft Victimization (n = 803)

	B	S.E.	Exp(B)	Sig.
Online routine behaviors				
Browsed the Internet	-0.571	0.259	0.565	0.027*
Used social media	-0.291	0.223	0.748	0.193
Purchased items online	-0.224	0.245	0.799	0.361
Stored digital information	0.243	0.198	1.276	0.218
Used cryptocurrency	0.492	0.169	1.635	0.004**
Surfed the Darkweb	0.634	0.193	1.886	<.001***
Online Guardianship				
Total online guardianship	0.257	0.093	1.294	0.006**
Computer skill	-0.162	0.181	0.850	0.369
Demographics				
Male	0.194	0.413	1.214	0.639
Black/African-American	-1.223	0.576	0.294	0.034*
Other race	-0.601	0.496	0.548	0.225
Hispanic	-0.067	0.487	0.935	0.890
Age	-0.052	0.014	0.950	<.001***
Education	-0.182	0.140	0.833	0.194
Income	-0.025	0.060	0.975	0.677
Constant	1.282	0.984	3.602	0.193
Chi-square (df)	121.703 (15) ***			
-2LL	279.353			
Nagelkerke R^2	0.358			

Note: *p<.05, **p<.01, ***p<.001