

Identity Theft and its Effects on Victims, Commerce, and Society: Ideal Systematic Approach  
Combating Identity Theft Involving a Combination of Prevention, Education/Outreach,  
Detection, Recovery, and Enforcement Components.

Approved by: *Dr. Cheryl Banachowski-Fuller*

April 12, 2022

Identity Theft and its Effects on Victims, Commerce, and Society: Ideal Systematic Approach  
Combatting Identity Theft Involving a Combination of Prevention, Education/Outreach,  
Detection, Recovery, and Enforcement Components.

Senior Seminar Research Paper Presented to the Graduate Faculty

University of Wisconsin – Platteville

Partial Fulfillment of the Requirements for the Master of Science in Criminal Justice

Jeffrey W. Hole

May 2022

### **Acknowledgements**

*I would first like to thank my wife, Victoria, for her encouragement and support for me for my ideals, my work, and my pursuit of my educational goals. Although these educational goals have always been “bucket-list” goals for me, she made those hopes an opportunity for achieving the reality. It has been almost a decade now since I had returned to school, and it was through her faith that I was able to earn my undergraduate degree, something I had meant to do for decades. With her support, I now work to complete the requirements for my graduate degree in Criminal Justice. That being said, I also want to thank my children Logan and Ivy for their understanding in having to sacrifice time with their Dad so that I could complete schoolwork over those many years. I would like to thank my colleagues at work, especially my superiors from both my current work unit as well as my previous one, which would include Robin Jacobs, Director of the Enforcement Bureau of the Wisconsin Division of Securities, Lutfi Shahrani and Amy Banicki, both formerly Directors of the Wisconsin Unemployment Insurance Division, and Jason Schunk, who was previously my direct supervisor during my time at the Unemployment Insurance Division. Each of them provided opportunities for me and supported my education efforts tremendously over the years. I would like to conclude with offering my gratitude and sincere thanks to Dr. Banachowski-Fuller as well as the instructors I had the opportunity to interact with throughout my time as a student of UW-Platteville’s graduate program in Criminal Justice. Each person provided me opportunities to learn and grow not just within the confines of our program, but as a person, through instilling a greater perspective of our Criminal Justice system and the roles we play as part of it to benefit our society.*

### **Abstract**

This paper explores and investigates identity theft through a compilation of statistical data and previous studies conducted regarding typical methodologies used, the effects of identity theft, and to develop ideal program components to provide services for the prevention, investigation, and resolution of identity theft incidents. The research examines both mundane methods (e.g., hardcopy records, checks, false identification cards, etc.) involved in the commission of identity theft as well as the use of cybertechnology (e.g., computers, devices, internet, electronic data storage, etc.) as the methods of operation. This research paper examines instances of known losses and harm suffered by individuals, businesses, and our society, as well as how law enforcement is challenged by this type of fraud within the United States. Based on previous studies conducted as well as both qualitative and quantitative (e.g., crime statistics) data available from law enforcement and regulators specializing in such investigations, the author explains the need for aggressive enforcement concerning identity theft and provides recommendations for components for a program to support such efforts. The author suggests possible future research improvements by addressing the need to obtain more specific and accurate data concerning identity theft incidents by jurisdiction as well as investigation, arrest, and prosecution outcomes. The author contends that improved data regarding types of identity theft may be obtained via additional and more recent cybercrime schemes and incidents of identity theft.

**TABLE OF CONTENTS**

APPROVAL PAGE ..... 1

TITLE PAGE ..... 2

ACKNOWLEDGEMENTS ..... 3

ABSTRACT ..... 4

TABLE OF CONTENTS ..... 5

I. INTRODUCTION ..... 8

    A. Statement of the Problem ..... 8

        i. There is a need for a consistent law enforcement and/or government program with baseline components fostering a multi-facet approach for combatting identity theft.

    B. Purpose of the Study ..... 9

        i. To determine ideal components for a model program via exploration of the problem based on: data from and evaluations of pre-existing programs; crime data; previous studies and literature to potentially reduce identity theft and increase effectiveness of victim assistance efforts.

    C. Significance of the Study ..... 10

        The current state of program efforts of our law enforcement and government agencies to handle Identity Theft issues appear to be more focused on prevention efforts on the part of potential victims as opposed to deterrent effects of potential accountability via enforcement for offenders. This is evidenced by shifts in resources and government programs over the past decade (e.g., dissolution of Wisconsin’s OPP and the fact that the CP program now solely provides victim assistance – no investigation or enforcement). Similarly, in Wisconsin most police departments take a report and provide information for victim assistance (e.g., Madison Police Department, Madison, WI). There are few prosecution referrals in comparison to instances of identity theft (reported vs unreported). There are a limited number of programs which combine a strategy of prevention, victim assistance, and enforcement to combat identity theft, and creating a model program incorporating such a multi-faceted approach may potentially reduce identity theft.

    D. Contributions to the Field ..... 11

II. Literature Review ..... 12

    A. Research Definitions ..... 13

        i. General Types for Identity Theft ..... 13

        ii. As Part of a Larger Scheme ..... 16

        iii. Source Funding for Criminal Enterprises and Terrorism ..... 17

- B. Role of Technology, Cybercrime, and Identity Theft.....18
  - i. Common Schemes .....19
  - ii. Case Studies .....20
  - iii. Jurisdictional Issues .....21
- C. Statistics for Reported Crimes of Identity Theft .....24
- D. Law Enforcement and Government Agencies .....26
- E. Effects on Businesses, Commerce, and Economies.....27
- F. Effects on Individual Victims .....28
- G. Enforcement vs. Business Practices.....31
  - i. How Fear of ID Theft impacts Commerce
  - ii. Taxes, Capital Loss Claims, Reduced Operating Revenue for Government
- H. Therefore, there is a need for a program to combat identity theft and safeguard our citizens, businesses, and government institutions.....35
  
- III. Theoretical Framework.....38
  - A. Social Contract Theory .....38
  - B. Social Control Theory.....42
  
- IV. Program Evaluation: Current Practices for Identity Theft Enforcement efforts and/or Prevention and Education/Outreach Programs .....45
  - A. Current Law Enforcement Practices in Wisconsin for Handling of ID Theft Complaints .....47
  - B. Current Methods and Strategies Employed by Government Agencies .....48
  - C. Current Strategies Employed by Private-Sector Businesses.....48
    - i. Enforcement vs. Business Practices
    - ii. How Fear of ID Theft impacts Commerce
    - iii. Taxes, Capital Loss Claims, Reduced Operating Revenue for Government
  - D. ID Theft Victims (General, Youth, and Elderly) .....50
  - E. Current State – Prevalent Programs .....52
  - F. Cause and Effect: Social Harms Inflicted from ID Theft Crimes.....56
  
- V. Recommendations.....57
  - A. Presentation of Statistical Evidence for Better Understanding of the Problem
  - B. Ideal Components for Program Overview .....59
    - i. Prevention and Security
    - ii. Public Outreach and Education
    - iii. Victim services and recovery efforts on behalf of victims
    - iv. Enforcement efforts
      - 1. Investigation
      - 2. Civil legal action
      - 3. Criminal prosecution
  - C. Data Breaches & Security Awareness .....67
    - i. Current Legal Obligations and Liability
    - ii. Suggested Reporting Mechanisms
    - iii. Private Sector Partnerships with Regulators

VI.	Conclusion .....	68
	A. Limitations .....	70
	B. Future Research .....	71
VII.	Reference List .....	72

## INTRODUCTION

### I. Introduction and Statement of the Problem

Identity theft has become a more common and substantial threat to commerce, economies, and the well-being of our people, businesses, and government institutions in the United States over the past decade (Zaiss, Zaeem, & Barber, 2019). Identity theft impacts citizens from all walks of life in multiple ways that include: damage to an individual's name and reputation; service and financial account takeovers; credit card fraud and fraudulent transactions; medical fraud, tax fraud, and putting retirement accounts at risk (Schultz, 2018).

Studies over a number of years (Lane & Sui, 2010; Schultz 2018) indicate a growing trend in identity theft (Chorghe, Jain, Mali, & Gunjgur, 2020), including an expansion of computer and internet technologies use (cybercrime) to perpetrate such crime (Van de Weijer, Leukfeldt, & Bernasco, 2019). These studies, as well as data obtained by both public and private sector organizations, suggest a need for increased effectiveness for programs concerning prevention and enforcement in response to identity theft crimes.

It has been argued that crimes of identity theft have a substantial and detrimental impact on commerce, (Shareef, Dwivedi, Kumar, Davies, Rana & Baabdullah, 2019), especially internet transactions, as well as inflicting psychological harm on individual victims of the crime (Golladay & Holtfreter, 2016). Most models used by law enforcement and government agencies, businesses, and other organizations operate with a focus on prevention and victim recovery (Federal Trade Commission, Consumer Information, accessed 2021), while enforcement and prosecutions actions lag by comparison (Uniform Crime Reporting, accessed 2021).

Some research suggests that a lack of criminal enforcement and prosecution emboldens criminals, and bad actors consider identity theft as lower risk and higher reward in comparison to

other criminal efforts intended to result in financial gain (Gupta & Kumar, 2020). Research further indicates that crimes of identity theft are often methods of source funding for organized crime and terrorism (Gupta & Kumar, 2020).

Combatting identity theft on all levels should be a focus for law enforcement, government agencies, and businesses throughout the United States. Not only do the efforts to combat identity theft serve our citizens in the immediate incident(s), but in considering a larger scope, combatting identity theft also simultaneously attacks the revenue streams funding organized crime and terrorism.

**a. Purpose of the Study**

The purpose of this research paper will be to explore and compare previous studies conducted on the scope and nature of identity theft crimes in the United States as well as past and current programs and strategies for combatting identity theft from a variety of sources. Programs and enforcement efforts generally appear ineffective in consideration of the growing trends of increases in Identity Theft. This research project will examine pre-existing programs on the federal, state, and local public sector levels as well as those of private industry (e.g., credit card, banking, insurance industry, etc.). The intent of the research project is to identify areas for improvement as well as make recommendations for an ideal approach combining identity theft prevention, detection, investigation, and enforcement options.

Additionally, the research will also explore cybersecurity/records security and how data breaches contribute to the victimization of citizens, businesses, and government organizations. Based on this research, suggestions will be given regarding prevention, security, and countermeasures regarding breaches and correlated identity theft activities.

**b. Significance or Implications of the Study**

This research paper will present arguments for an aggressive multi-faceted approach to combat the crime of identity theft that includes but is not limited to increased prevention, education, and enforcement efforts. In consideration of annual losses suffered by individuals, businesses, and our government institutions, the costs for aggressive approaches to combatting identity theft should be negligible.

This research paper will present the argument that a failure to take a more aggressive approach to combatting identity theft potentially emboldens bad actors and increases the amount of the crime suffered by the community (local, regional, and national). Continued trends of increases of identity theft crimes will inflict great economic harm upon individuals, institutions, and society as a whole, and identity theft is a means used by bad actors as a part of greater and more sophisticated fraud schemes to fund greater criminal enterprises and terrorism (Gupta & Kumar, 2020).

There is currently little literature exploring the combination of prevention, victim recovery, and enforcement/deterrence approaches of combatting identity theft crime. Much like a medical treatment for a disease (Burnes, DeLiema, & Langton, 2020), each facet serves a specific purpose to comprise an overall strategy to increase effectiveness combatting identity theft via a combined effort. By establishing a basic model to combat identity theft, law enforcement, government agencies, and our businesses can benefit from the cooperative efforts involved.

**c. Methods of Approach**

A secondary analysis of previous studies, articles, and literature will be the primary

research method used in this research paper. Statistics will be gathered from government agencies (e.g., Uniform Crime Reporting, Wisconsin Department of Justice, Federal Trade Commission, and the Wisconsin Bureau of Consumer Protection) regarding reported incidents of identity theft. Information obtained will be explored to determine a conclusion of both historical trends and our current status in order to provide recommendations for potential future program initiatives and strategies to combat identity theft and prioritize the allocation of resources for optimal effectiveness.

A combination of quantitative and qualitative data will be gathered and analyzed to determine if reported incidents of identity theft have increased or decreased over the past decade. Qualitative data will include reports of incidents designated as identity theft combined with other reported crimes that may have been reported as another related type of crime designation (e.g., credit card fraud, social media hacks, etc.), but could also be defined as forms of identity theft, nonetheless. Quantitative data will be sought of reported crimes in consideration of population data to determine if identity theft is increasing or decreasing not just in the amounts of reported incidents, but per capita as well.

#### **d. Contribution to the Field**

The primary contribution to the research will be recommendations for best practices and guidelines for programs that combat identity theft. Best practice recommendations will be based on the information obtained during the research, and will involve the recommendation of a multi-faceted approach for regulators and law enforcement to combat identity theft that includes a combination of: Education & Outreach; Deterrence and Prevention; Enforcement & Investigation; and Enforcement & Prosecution.

Currently, most programs to combat identity theft involve approaches limited in scope to the role or mission of the organization (e.g., law enforcement handle complaints and investigate matters, credit card companies correct billing issues related to fraudulent transactions, regulators focus on victim assistance efforts, etc.). While these efforts certainly provide value, current trends arguably question their overall effectiveness in reducing crimes of identity theft overall. The contribution of a program model incorporating the proposed multi-faceted approach could potentially reduce incidents of identity theft crimes, thwart larger scale financial crimes/terrorism that rely on identity theft as a funding source, and strengthen cooperative relationships between law enforcement, businesses, and community members. There are a limited number of programs that combine all the approaches, so a best-practices recommendation incorporating multiple approaches may provide a substantial and relevant contribution to the field.

## **II. Literature Review**

This research paper's literature review is separated into eight (8) topic segments as follows: 1) commonly held definitions for forms of identity theft as well as semantical types and legal definitions; 2) identity theft as a method of funding for organized crime and terrorist activities; 3) the role of technology and forms of cybercrime used in the commission of identity theft, followed by an exploration of related case studies and potential jurisdictional issues faced by law enforcement; 4) statistics for reported cases of identity theft in Wisconsin and nationwide; 5) the role and efforts of law enforcement and government agencies regarding identity theft; 6) the effects of identity theft on businesses, economies, and individual identity theft victims; 7) the interrelationships and conflicts between law enforcement efforts and business practices; and 8) the findings resulting from the literature review supporting the need for government programs to combat identity theft and protect our citizens, businesses, and economies.

## Research Definitions

### *General Types for Identity Theft*

According to the definitions and statistics of both the Federal Trade Commission (Retrieved February 12, 2022) and the Federal Bureau of Investigation (Retrieved February 12, 2022), identity theft ranges from acts as simple as a person orally providing a another's name to the authorities as their own to evade accountability, to activities using more complex methods such as cyber-technologies to hack into the bank account of another person to drain funds from the account(s). In decades past, incidents of identity theft would typically involve altered or falsified hardcopy documents, forged checks, or fake identification cards. However, while such incidents do still occur, technology has made those methods appear obsolete. Today, crimes involving forms of identity theft typically also involve the use of computer and cyber technologies. According to the Wisconsin Department of Agriculture, Trade, and Consumer Protection's identity theft information (Retrieved February 12, 2022), such instances typically involve cybertechnology as the method or means for a bad actor to obtain the identity or identifying information of another through activities such as phishing, digital data theft, computer intrusions. In addition, cyber technology is often used to perpetrate identity theft during the commission of other schemes or crimes, such as obtaining goods or services as an imposter and under false pretenses (e.g., avoiding legal process, establishing financial accounts, service accounts, or social media accounts, obtaining employment and obtaining medical services).

While nuanced legal definitions of identity theft may vary between jurisdictions, the general understanding of actions defined as identity theft involve the use of an individual's personally identifying information by another and without the consent of that person. This

involves an imposter pretending to be the other person to obtain a form of benefit or gain at the expense of the individual being impersonated, typically for financial gain or to avoid legal process. This research relies, in part, on legal definitions per Wisconsin law and federal law specific to identity theft.

Wisconsin law defines identity theft, in part, as follows:

Wis Stat. 943.201 (retrieved February 2022) – *Unauthorized use of an individual's personal identifying information or documents*. The statute defines how jurisdiction is determined and provides statutory definitions for the meanings of terms such as “personally identifying information” and “personally identification document”. Wisconsin’s statute further defines what acts constitute forms of identity theft, in part, as follows:

(2) Whoever, for any of the following purposes, intentionally uses, attempts to use, or possesses with intent to use any personal identifying information or personal identification document of an individual, including a deceased individual, without the authorization or consent of the individual and by representing that he or she is the individual, that he or she is acting with the authorization or consent of the individual, or that the information or document belongs to him or her is guilty of a Class H felony:

- (a) To obtain credit, money, goods, services, employment, or any other thing of value or benefit.
- (b) To avoid civil or criminal process or penalty.
- (c) To harm the reputation, property, person, or estate of the individual.

Wis. Stat. 943.203 (retrieved February 2022) – *Unauthorized use of an entity's identifying information or documents*. This statute provides definitions of terms such as “entity” and “identification document”, and further defines jurisdiction. The statute defines what acts are forms of this type of identity theft, in part, as follows:

(2) Whoever, for any of the following purposes, intentionally uses, attempts to use, or possesses with intent to use any identifying information or identification document of an entity without the authorization or

consent of the entity and by representing that the person is the entity or is acting with the authorization or consent of the entity is guilty of a Class H felony:

- (a) To obtain credit, money, goods, services, or anything else of value or benefit.
- (b) To harm the reputation or property of the entity.

Federal law defines the federal crime of identity theft, in part, as follows:

18 U.S.C § 1028 (retrieved February 2022) – *Fraud and related activity in connection with identification documents, authentication features, and information.*

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

- (1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;
- (2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;
- (3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;
- (4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;
- (5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;
- (6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

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

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

### ***As Part of a Larger Scheme***

As indicated by Gupta & Kumar (2020), activities that may be defined as forms of identity theft frequently may either lead to additional financial crimes and forms of identity theft, or also be an element of a greater fraudulent scheme that makes use of false information, fictitious financials, forged documents, false references, or similar such dishonesty. A common example of such a scheme would involve an individual acting as an imposter and using the identifying information of another person during their efforts to obtain employment and other additional benefits, such as health insurance offered via the employer, financial loans, credit lines or credit cards relying on the illegitimate employment information, etc. In this example, the fraudulent scheme involves an imposter obtaining employment and continuing the scheme by obtaining additional goods or services that are predicated upon that imposter's fraudulently obtained employment.

The Federal Bureau of Investigation's *Financial Crimes Report to the Public Fiscal Year 2008* (Retrieved February 19, 2022) indicates that various forms of corporate misconduct, including forms of identity theft and falsified records, contributed to the 2008 economic and financial crisis suffered by the United States. Fligstein & Roehrkasse (2016) indicate that malfeasance regarding mortgage-backed securities and associated mortgage fraud schemes inflicted harm on local, state, national, and global economies, and that such schemes involved a combination of a pervasive culture present within the industry and underlying financial crimes

and fraud. Mortgage fraud is no different than other fraud schemes, in that most of such crimes also involve forms of identity theft in order for the perpetrator(s) to carry out the overarching fraud scheme, especially when forged documents, imposters and straw buyers are used in commission of the crime(s). The financial crash of 2008 has influenced our political and corporate culture within the United States since then, resulting in proposed legislation and arguments for the need of increased regulatory oversight of our financial industry.

### **Source Funding for Criminal Enterprises and Terrorism**

According to Hill & Marion (2016), Presidential speeches have involved rhetoric on cybercrime and activities that threaten the public, and that such rhetoric is used to motivate the population and evoke fears from the public to influence the public perception of the crime itself for the purpose of obtaining political or legislative support. Hill et al. assert that cybercrime has been linked to national security and terrorism in such rhetoric to bolster the public's perception that cybercrime is a mechanism that funds terrorist activities that threaten them. Hill et al. does not characterize the rhetoric as untrue, but rather that it has been historically used for supporting an agenda.

A study conducted by Leukfeldt, Kleemans, Kruisbergen, & Roks (2019) utilized empirical data to explore the use of cyber technologies by organized crime groups through a comparison of thirty (30) investigations of organized crime groups ranging from those involved in low-tech use schemes to schemes using complex technologies. Leukfeldt et al. concluded that although some level of a localized presence was maintained in each case that was analyzed, cybercrime provided opportunities for organized crime groups to expand their fraudulent activities beyond traditional borders of their geographical area.

A study conducted by Jian, Chen, Luo, Lee & Yu (2020) analyzed eighty (80) prosecuted cases of cybercrime using a grounded theory approach to determine that the cyber criminals of organized crime groups utilize a systematic approach to use internet technologies to victimize individuals and businesses for financial gain. Jian et al. further label these cybercrimes as a form of “racketeering”, and indicate that the activity poses a serious threat to nations as well as to entities and individuals.

### **Role of Technology, Cybercrime, and Identity Theft**

Gupta & Kumar (2020) indicate identity theft via cybercrime is the most common form of this type of fraud occurring today. Electronic communications (e.g., cellular telephone, internet, etc.) are now the primary form in which people routinely transact business from day to day. Financial transactions (routine banking, investments, etc.) are commonly performed via internet or through use of a personal cellular telephone. Gupta et al. indicate that criminals perpetrating identity theft also use that technology to intrude into our databases, intercept our transmitted communications, and obtain our personally identifiable information to further use that information to make fraudulent purchases or establish fraudulent accounts.

Chawki, Darwish, Khan, & Tyagi (2015) indicates that advances in internet, computer, and information technologies have impacted global interconnectivity and commerce while simultaneously expanding the ability of criminals to victimize others via cybercrimes and identity theft.

The Bulgarian study of Georgiev (2019) describes the benefits in advances in information technology and the prevalent use of those technologies in our everyday lives. Georgiev further indicates that with the advances in information technology, criminal activities have simultaneously expanded through cybercrime making use of the same technologies. Utilizing

both inductive and deductive methods, Georgiev then explores the human roles involved with cybercrimes, including the cybercriminals, victims, and investigators or law enforcement officials. Georgiev concludes that profiling practices are also useful when considering cybercrime, and that prevention practices could be developed when enough data has been obtained.

In their study, Tcherni, Davies, Lopes & Lizotte (2016) contend that despite a recorded drop in general crime since the 1990s according to Uniform Crime Reports of the Federal Bureau of Investigation, available data indicates that online property crime have increased. Tcherni et al. explores both the data for reported crime and the reporting mechanisms for crime, and suggest that an increasing trend in cybercrime exists that is not accurately reported. Using a combination of data from the Federal Bureau of Investigation and other multiple sources regarding “Online Property Crimes”, Tcherni et al. found again that while reported incidents of traditional property crimes have declined, online crimes have dramatically increased.

### ***Common Schemes***

According to a study conducted by Holt & Bossler (2014), the most common cybercrime schemes (including forms of identity theft) include the following categories:

Cyber-Trespass – commonly known as hacking or computer intrusion, these activities involve an unauthorized entry into the computer, network, or data source of another. These activities may be initial steps toward inflicting other harms during the commission of other forms of cybercrime.

Cyber Deception/Theft – The actions of this category involve various forms of identity theft and imposter activities to commit financial crimes and fraud, but also includes the use of

cyber technology for digital piracy, or to steal information, data, or anything of value from victims.

Cyber Porn and Obscenity – This category of activities involve the communication, transmission, and distribution of sexually explicit materials, including crimes against children.

Cyber Violence – This category involves ways in which harm can be inflicted upon others in either real or virtual environments. Examples of such activities include, but are not limited to cyber stalking, bullying, harassment, doxing, threats to injure or cause harm, incitement of others to commit acts of violence, and the organization and incitement of violent actions targeting political groups and governments. Other forms of cyber-violence include the introduction of malware, computer viruses, spyware, or other malicious programming to harm the computer or data systems of another.

### *Case Studies*

The study of Jakubiec (2020) from Poland addresses multiple forms of identity theft and argues that the demographic most at risk for becoming victims of identity theft are our elderly, as they are typically unaware of basic security precautions regarding internet use and safeguarding their documents and identity information. Jakubiec also asserts that risks are associated with data stored on electronic media that are integrated into internet access (e.g., the Cloud or other internet platforms).

Hille, P., Walsh, G., & Cleveland, M. (2015) indicate in their study through the use of quantitative data from Germany and qualitative data from interviews that an increase of e-commerce or online shopping increases consumer fear of their risk of becoming victims of identity theft. Hille et al. indicate that as consumer sentiment is a driver for purchases and

transactions, fear of having their identifying information compromised impacts online commerce.

Maras (2016) conducted a study regarding partnerships between international jurisdictions for investigations of cybercrime and prosecutions of such matters. As an example of such a successful effort, Maras cites “Operation Shrouded Horizon” and the investigation of “Darkode”, an internet site serving as a platform in the sale of stolen data (e.g., personal identity information and financial information) as well as questionable goods and services (e.g., malicious computer programs and malware), whose contents were accessible only via password by established members. Maras indicates that the cybercrime investigation involved a partnership of investigators from 19 different countries and resulted in the arrest of about 70 “Darkode” members worldwide. Although Maras asserts that such an operation is not unique, she cites the operation as both a case study of the importance of multi-jurisdictional collaboration and example of a successful multi-jurisdictional cybercrime investigation that was global in scope.

The Australian study of Brown, C.S.D. (2015) makes use of a fictional circumstance of cybercrime as a case study to explore the barriers often encountered by law enforcement in investigating cybercrimes such as identity theft, and the difficulties regarding multi-jurisdictional and often global circumstances of the crimes creating limits of current criminal justice systems and practices to hold bad actors accountable.

### ***Jurisdictional Issues***

Although Susan Brenner went on to author many works used as collegiate academic textbooks, in her early work titled *Cybercrime jurisdiction. Crime, Law, and Social Change* (2006), she established a foundation for understanding identity theft, cybercrimes, and how such

matters may be investigated or resolved. Brenner (2006) indicates that establishing jurisdiction in an identity theft matter may be a barrier for law enforcement and investigators, especially if perpetrated as a cybercrime. While most criminal identity theft statutes establish jurisdiction for investigators and prosecutors' offices based on the residence of the victim within the jurisdiction in question, statutes for other criminal offenses that may apply to case circumstances (e.g., wire fraud, mail fraud, forgery, theft, etc.) may be less clear regarding how jurisdiction is determined, typically only when some material part of the transactions in question occurred within the jurisdiction. With criminal violations and cybercrime, some part of the activity or transaction must somehow involve the jurisdiction, such as victims, perpetrators, or the financial institutions being located within the jurisdiction. In consideration of cybercrime, emails or some form of electronic communication transmissions that either in whole or in part pass through an Internet Service Provider ("ISP") or mechanism located within a jurisdiction often establishes authority or jurisdiction over such a transaction. Brenner suggests that cybercrimes typically involve actors and victims from different sovereign states and present legal challenges for investigators and prosecutors. Other countries may have lower legal standards for evidencing a crime or have different rules of evidence not in alignment with those of the United States. As such, investigators must ensure that their work complies with multiple sets of legal standards for evidence and investigative methods. As implied in Brenner's work, investigators must not only form effective partnerships between jurisdictions, but must also educate themselves on the differences between jurisdictions and adhere to the strictest standards among the jurisdictions involved in a matter being investigated in order to collect and preserve evidence admissible for all potential prosecution efforts.

In an Australian study, Brown, C.S.D. (2015) indicates that there are barriers hindering the investigation and prosecution of cybercrimes, as many such incidents involving cybercrime involve actors spread throughout multiple jurisdictions, including throughout a nation or internationally. Brown explores how police agencies, government agencies, private sector businesses, and international relationships provide value and the means necessary to resolve matters of cybercrime and identity theft. Brown addresses the common law model that translates to most Western criminal justice systems, such as police conducting interviews of witnesses (e.g., victims, suspects, and third-party witnesses). Often, investigative efforts to obtain information or communicate with potential witnesses in a cybercrime or identity theft matter involve additional issues regardless of the establishment of proper authority and jurisdiction of the agency to investigate a matter, which includes access to witnesses involved and monetary costs associated with such access. Brown implies that such witness access can also be a barrier for prosecutors to obtain court testimony. Although monetary costs can be mitigated via technology as opposed to in-person meetings with witnesses, electronic telecommuting may be more difficult to present evidence or records with a witness for their review in comparison to doing so in person. Behavioral or psychological queues may be missed via electronic communications as opposed to in-person observations of a witness's body language. However, it is expensive to have witnesses from outside the jurisdiction to travel (when possible) to meet investigators or prosecutors, as it is likewise expensive for investigators to travel to meet witnesses outside of the geographical jurisdiction. Likewise, the same issues of expense apply to target witnesses/suspects that reside or are otherwise located outside of the geographical jurisdiction. For a suspect outside of the geographical jurisdiction to be arrested or physically taken into custody, additional legal issues complicate the process (e.g., extradition, other

jurisdiction recognizing authority of investigating jurisdiction, etc.).

In an early study, Bednar, Katos, & Hennell (2009) indicate that the collaborative approach between jurisdictions to investigate cybercrimes often involves conflict in the differences of investigative methods to obtain, maintain, and analyze evidence. Bednar, et al., indicate that the establishment of procedures to be commonly accepted and used between jurisdictions would be beneficial, and that in addition to defined procedural steps and methods, the logistics of assigned tasks of collaborating investigators between jurisdictions increases the efficiency and effectiveness of the investigation overall.

### **Statistics for Reported Crimes of Identity Theft**

Federal Bureau of Investigation (“FBI”) Uniform Crime Reporting (“UCR”) categories are not specific to identity theft. However, the FBI’s Internet Crime Complaint Center (“IC3”) does produce data regarding cybercrimes that are either forms of identity theft or related to identity theft. FBI data demonstrates that between the years of 2016 through 2020, IC3 received 2,211,396 complaint filings attributed to aggregate losses of approximately \$13.3 Billion. This data is reflected in Table 1 below:

***Table 1a: FBI Computer Crime Report Statistics per I3C for the United States***

Reporting Year	Total # Complaints	Dollars Losses - Billions	Average Loss per complaint
2020	791,790	\$4.2	\$5,304.44
2019	467,361	\$3.5	\$7,488.86
2018	351,937	\$2.7	\$7,671.83
2017	301,580	\$1.4	\$4,642.22
2016	298,728	\$1.5	\$5,021.29

\*data derived from <https://www.ic3.gov/Home/AnnualReports>

Table 1a demonstrates a pattern of increased incident reporting of cyber-related crimes via IC3, with monetary losses also increasing overall. However, while the average dollar amount of loss per report appears stable when comparing the years 2016 and 2020 (an average loss of \$5,162.87 per report for those two years), within the time span there was an increase in the average loss per

report of about \$1,500.00 suffered (an average loss of \$6,600.97 per report for the years of 2017, 2018, and 2019). Table 1b below further demonstrates a continual increase in reported identity theft via IC3 between the years of 2016 through 2020.

**Table 1b: FBI ID Theft Report Statistics per I3C for the United States**

Reporting Year	# Complaints ID Theft	# Complaints Data Breach	# Complaints Phishing, etc.	# Complaints Extortion
2020	43,330	45,330	241,342	76,741
2019	16,053	38,218	114,702	43,101
2018	16,128	50,642	26,379	51,146
2017	17,636	30,904	25,344	14,938
2016	16,878	27,573	19,465	17,146

\*data derived from <https://www.ic3.gov/Home/AnnualReports>

Other government agencies compile data specifically regarding reported forms of identity theft. According to Federal Trade Commission data (Retrieved February 12, 2022), reported instances of identity theft have steadily increased between the years of 2017 through 2021 for both the United States and the State of Wisconsin. This data is reflected in the Tables 2a and 2b below:

**Table 2a: Identity Theft Statistics per Federal Trade Commission for the United States**

Reporting Year	Credit Card Fraud	Other	Loan or Lease	Bank Fraud	Phone or Utilities	Employment or Tax-related	Government documents or benefits	Aggregate
2021	287,734	294,776	154,646	92,894	68,626	98,165	263,747	1,066,783
2020	393,345	353,405	205,066	89,612	99,579	113,593	406,566	1,387,594
2019	271,934	215,899	104,766	58,854	83,642	45,580	23,242	650,523
2018	157,745	122,668	51,943	52,616	63,660	67,291	24,959	444,339
2017	133,105	65,459	30,099	50,627	55,144	82,050	25,961	370,915

\*data derived from <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/IDTheftbyState>

**Table 2b: Identity Theft Statistics per Federal Trade Commission for the State of Wisconsin**

Reporting Year	Credit Card Fraud	Other	Loan or Lease	Bank Fraud	Phone or Utilities	Employment or Tax-related	Government documents or benefits	Aggregate
2021	1,511	2,043	1,061	887	499	1,135	2,389	8,289
2020	2,322	2,327	1,147	1,084	727	966	2,232	8,985
2019	1,936	1,500	731	666	668	432	218	5,023
2018	1,191	882	328	502	483	755	247	3,728
2017	1,397	581	280	494	453	859	229	3,735

\*\* data derived from <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/IDTheftbyState>

### **Law Enforcement and Government Agencies**

Literature findings demonstrate the complexities of addressing identity theft and cybercrime as involving relationships between law enforcement, government agencies, and businesses.

In an early study, Romanosky, Telang, & Acquisti (2011) indicate that about \$56 Billion USD in losses were suffered by consumers and the corporate sector in 2005, and that about 35% of known incidents of identity theft were prompted or caused by the data breaches of businesses. Romanosky et al. indicate that there had not been much empirical evidence at the time of their study to determine the effectiveness of data breach disclosures in reducing identity theft. Romanosky et al. made use of a Federal Trade Commission panel to obtain information and estimates, and explored the potential impacts that data breach disclosure laws have on identity theft crime rates. Romanosky et al. conclude in their findings that data breach disclosures reduced known identity theft incidents by about 6.1%.

Bisogni & Asghari (2020) conducted a study that explored the potential relationships between the occurrences of data breaches and incidents of identity theft, and the role of notification laws regarding data breaches. Bisogni et al. made use of empirical data and Bayesian modeling for a comparison between known data breaches and reported incidents of identity theft to determine that the activity was dependent upon the size of the state, and that data breach notification laws slightly reduced identity theft incidents.

According to Dupont (2016), the use of botnets in cybercrime represents the greatest threat to internet networks and what Dupont terms the “digital ecosystem”, which is inhabited by individual people and corporations alike. Dupont argues for the need of a multifaceted approach or “polycentric regulation” to be implemented for increased effectiveness in combatting forms of

identity theft and cybercrime (e.g., denial of service attacks, financial and bank fraud, and imposter click fraud). Dupont contends that the three most prominent strategies in use at the time of his study include: the arrests of pronounced cybercriminals by law enforcement to promote deterrence; Microsoft taking efforts to disrupt, interrupt, and ruin cybercrime botnet operations; and some nations encouraging the formation of partnerships between government entities and private-sector internet service providers, internet security software providers, and regulatory organizations. Dupont explores the need for such strategic efforts to destroy or disrupt the cybercrime bot networks and to reduce the harm inflicted by them, as well as the current limitations suffered by law enforcement to address cybercrimes. Dupont reported that serious consideration of formalized programs and implementation of aggressive ongoing strategies were being initially considered by regulatory authorities at the time of his study.

### **Effects on Businesses, Commerce, and Economies**

The work of Barnett-Ryan, C. (2002) regarding the measurement of white-collar crime using data from the Federal Bureau of Investigation's Uniform Crime Reporting ("UCR") data has been cited and repeated throughout the years. Although the Federal Bureau of Investigation compiles and tracks crime data via the UCR, according to Barnett in a recent publication via the FBI (2018), the scope of harm and actual losses suffered by victims of white-collar crime are not known, and can only be estimated based on available data.

In its 2020 Internet Crime Report (Retrieved February 22, 2022), the FBI attributes an estimated \$4.2 billion in losses to cybercrime. The 2020 Internet Crime Report further indicates that about 42% of computer crimes are categorized as larceny type offenses (which would typically involve some form of identity theft). The report does not, however, account for other harms inflicted or losses suffered by cybercrime and identity theft victims, such as lost time or

wages spent in recover efforts, or potential medical expenses associated with resulting mental health issues.

Kumar & Shareef (2012) indicate in their study that although online purchase transactions are not the cause or source of the majority of identity theft issues, consumer fear of identity theft has a significant impact on the purchase intention of consumers via online purchases or E-Commerce. Jordan, Leskovar, & Marič (2018) conducted an online survey of 190 Slovenian consumers to determine how fear of identity theft may impact the online purchasing activities of consumers and resulting consumer purchasing practices impacts on business. Within the context of the surveys, Jordan et al. focused on the concepts of consumer fears of: financial losses; damage to reputation; perceptions of risk; and online purchase intention. Jordan et al. found that the fear of identity theft increases the perceived risk in a consumer, which in turn reduces the online purchase intention or the probability of a consumer making an online purchase. Jordan et al. concluded that online businesses should adjust their business practices to address the concerns and perceptions of consumers to mitigate their fears of identity theft to improve sales and profitability.

### **Effects on Individual Victims**

According to the Wisconsin Department of Agriculture, Trade and Consumer Protection (February 12, 2022) as well as the Federal Trade Commission (February 12, 2022), identity theft has become a common means for the commission of various cybercrimes, and is generally associated with financial crimes (e.g., fraudulently obtaining a mortgage or loan via use of the identity of someone more creditworthy). Identity theft is also be attributed to instances of someone avoiding legal process, or obtaining goods or services that he or she would not otherwise legitimately be able to obtain. Victims of cybercrime and identity theft suffer harm

that includes: an inability to obtain loans, services, or goods because of damaged credit standing; being billed or charged for debts that they did not incur themselves; tax issues and debts caused by an imposter; being falsely blamed for a crime committed by an imposter; and inaccurate medical records when medical services were obtained by an imposter. Harm inflicted upon the victim can range from the inconvenient (e.g., unauthorized credit card charges) to deadly (erred medical diagnosis based on incorrect medical records).

Kerstens & Jansen (2016) indicate in their study that an overlap frequently exists between the crime victim and the perpetrator within the scope of cybercrime, and that the rate or trend of such an overlap or correlation existing is similar to other general crime trends. The study of Kerstens et al. is limited to a sampling of 6,299 Dutch juveniles between the ages of 10 and 18, and suggests that contributing factors to incidents were motivations of revenge and lower self-control.

The study of Navarro & Higgins (2016) suggests that with the increase of identity theft incidents overall within the United States for the past two decades, incidents of identity theft perpetrated by family members is also likely to increase. Using data from the 2012 (January – July) National Crime Victimization Survey, the study differentiated incidents of identity theft between non-familial relationships between victim and perpetrator and those incidents involving familial relationships, and found that identity theft involving family members victims occurred more often than those of non-family victims. However, Navarro et al. also indicates that there are few predictors for who may become victim of identity theft, and that detecting fraud committed by family members is difficult. Navarro et al. indicated that family-member identities were typically fraudulently used for obtaining government benefits or driver's licensing. Imposters using the identity of children may do so to establish credit, obtain goods/services,

circumvent legal process (e.g., civil actions, child support, law enforcement inquiries, etc.), or to escape any stigma attached to their own name (e.g., controversies, criminal convictions, etc.).

A difference between adult victims and juveniles is that the identity theft may go undiscovered until the victim turns age 18, applies for loans, or applies for college funding programs. In contrast to the study of Navarro et al., a study conducted by DeLiema, Burnes, & Langton (2021) explore the victimization of our elder adults by imposters, where a financial loss impacts a retired person's ability to pay the costs their own medical treatments, utilities, or even housing. The study of DeLiema et al. asserts that less affluent older victims of identity theft experience more emotional distress than wealthier victims, and that disadvantaged older adults living in poverty were more likely to suffer additional costs due to victimization and to struggle for recovery.

In addition to financial losses suffered and loss of time spent to recover an identity and repair damages resulting from identity theft, psychological harm is also inflicted on victims. Golladay and Holtfreter (2016) indicate in their study that victims of identity theft suffer both emotional and physical distress resulting from the theft of their identities, including issues of depression and declining general health. Golladay et al. asserts that victims report a sense of loss, betrayal, shame, helplessness, and anger in response to identity theft victimization. Identity theft victims lose their confidence as consumers regarding the safety of their information, resulting in a reduced likelihood of people making purchases or investments after suffering victimization.

The Australian study of Cross, Richards, & Smith (2016) regarding reporting and support needs of cybercrime victims focused on obtaining information about: the harm experienced by cybercrime victims; why some people chose to report the crime; and how best to meet the

support needs of victims. Cross et al. interviewed 80 adult victims ranging between 30 and 77 years in age to make inquiries about the effects online fraud had on them, including psychological or emotional impact. Cross et al. found that victims reported feelings of anger, shame, sadness, depression, and distress. In some instances, victims reported the experience as “soul-destroying” or having suffered a form of nervous breakdown. Cross et al. indicated that in some instances fraud victims contemplated suicide, suffered issues in personal relationships, or suffered physical ailments and insomnia. Cross et al. indicate that such emotional distress creates barriers for crime victim reporting. Cross et al. conclude that a primary concern for victims is the need to be heard and be regarded with respect and to obtain open and honest support from friends, family members, and organizations assisting them.

### **Enforcement vs. Business Practice**

Trost (2017) asserts in her work that an inherent conflict exists between fraud prevention efforts and the regulation of commerce. Trost indicates that the regulation of commerce in the United States is primarily focused on promoting movement of capital, money flows, and financial transactions. This is done in the United States, Trost states, “even in the face of unfairness or fraud”. Trost argues that this circumstance enables imposters and identity thieves to more easily operate than if priorities were reversed and reflected in our laws and regulation of commerce and the financial industry. Trost cites examples of such regulated practices, such as a signature not being required for instances of credit card transactions under \$50.00, and argues that while financial institutions are able to absorb losses occurring from identity theft as a cost of doing business or pass those losses on to consumers (e.g., increased service costs, etc.), problems of identity theft and fraud will continue for individuals as well as the general public.

In an article published in *Business and Society Review*, Payne & Kennett-Hensel (2017) explore identity theft and its effects on those involved, including the businesses involved in fraudulent transactions to determine recommendations to combat identity theft. Payne et al. explore laws regarding both the rights of identity theft victims and the obligations of other parties involved (e.g., businesses that transacted with the imposter). Payne et al. argue for the need of ethical business practices to prevent or mitigate identity theft, and further indicate that as members of society, individuals and businesses have legal and moral obligations to be aware of and take action to prevent identity theft.

### ***How Fear of ID Theft impacts Commerce***

Kumar & Shareef (2012) indicate that fear of identity theft or exposure to circumstances that may put the consumer at risk is a factor for consumers when considering whether to make online purchase transactions or otherwise participate in forms of e-commerce.

Apau & Koranteng (2019) of Ghana indicate in their study that cybercrime and the vulnerability of economies have increased in parallel with the increased use of internet technologies in business around the world. Apau et al. conducted a survey of 476 consumer participants and indicate that cybercrime and the fear of being compromised by it have impacted consumer trust, and contend that cybercrime poses a serious threat to e-commerce. Apau et al. indicate that as of the date of their study, Africa has experienced a severe increase in cybercrime activities that include financial and identity fraud, money laundering and financing terrorism, and human trafficking. Apau et al. contend that losses from cybercrime hinders the economy of Ghana. Apau et al. explore international commerce as well, and indicate that identity theft and cybercrime cause businesses to suffer losses of sales income due to reduced consumer confidence. Apau et al. conclude that consumer confidence for e-commerce would increase

when businesses improve privacy and security features of their own systems. Apau et al. also suggest a need for the creation of technologies to enable offenders to be identified and punished, and that doing so should cause a reduction in any poor perceptions or fears consumers may have regarding e-commerce.

### ***Taxes, Capital Loss Claims, Reduced Operating Revenue for Government***

Advances in cybertechnologies have served to increase the ease in which we conduct transactions, but arguably also have expanded the ways fraud can occur through use of those same technologies. Leighton-Daly (2019) explores this occurrence in the context of identity theft and tax crimes within Australia. Leighton-Daly examines technology-based fraud detection systems, and how existing Australian law can promote the detection, investigation, and prosecution of identity thieves committing such fraud. Leighton-Daly concludes that even sophisticated cybercrime fraud schemes making use of taxpayer information can be thwarted by well-resourced organizations.

Yenouskas & Swank (2018) explore the legal issues and lawsuits associated with data breaches suffered by businesses, organizations, and government entities, as well as the costs to mitigate those breaches of the personally identifying information of others. In most instances, forms of credit monitoring are provided to the victims of such data breaches at the cost of the entity breached. Yesnouskas et al. additionally explore instances and resulting litigation regarding the filing of false tax returns, or a citizen's own legitimate tax filings being compromised by the earnings or actions of an imposter using their information. Yesnouskas et al. further imply that in addition to the government suffering losses due to the costs associated with the time and expense of correcting the issues involving imposters filing tax returns, a loss of tax revenue on the earnings of the imposter also occurs.

Tax revenue based on individual citizen income(s) is based on capital gains on investment accounts in addition to income obtained via employment salaries. Schultz (2018) indicates that cybercriminals and fraudsters are targeting 401(k) and Individual Retirement Accounts (“IRA”) of individuals because of the typically larger amounts of money involved, and asserts that an upsurge in identity theft incidents places such accounts at risk. Schultz argues that financial industry professionals need to be diligent to deter, detect, and prevent such fraud from victimizing their clients. Schultz indicates several common instances of fraud targeting IRAs as involving: email account takeovers; phishing encounters; social engineering efforts (e.g., trickery or psychological manipulation to obtain identity information; malware; spoofing (impersonation of person or individual to prompt someone into providing their ID information); credential replay (ID thieves obtaining information because account holder uses same user name and passwords on multiple websites); or call forwarding (when ID thieves fool the victim’s telecommunications service provider to forward calls to the number of the bad actors). Schultz contends that firms possess a degree of legal liability in protecting clients from identity theft and account takeovers, and provides examples of protections that should be commonly used that include: communicating with the account holder by telephone to confirm online distribution or funds transfer requests; notifying account holder via hardcopy mail of any changes made to an account; making all distributions via hardcopy check; requiring approval from employer for distributions (applicable in some cases depending on IRA account); blocking suspicious IP addresses and requiring follow-up with the account holder; and placing restrictions on account distributions for a number of days or weeks following an account change or unusual activity being detected. Schulz concludes that while recordkeepers and account managers have a degree of responsibility

to protect clients from identity theft and fraud, the account holders also need to be responsible in safeguarding their own accounts.

Collectively, the studies of Leighton-Daly (2019), Yenouskas & Swank (2018), and Schultz (2018) highlight impediments for national, state, and local governments to obtain and make use of tax revenue used to fund government services and programs (which include efforts to combat identity theft and cybercrime).

### **Need for Program**

In their study, Graves & Sexton (2017) argue that successfully combatting trends in increasing identity theft requires stronger laws (and implying, by extension, enforcement of those laws). Graves et al. indicates that (as of the time of their study), at least 7% of the American population that is 16 years of age or older have been known victims of some form of identity theft, with resulting financial harm to be estimated at about \$15 billion USD in annual losses. Graves et al. argue that rising incidents of identity theft combined with the rising burden and costs for monitoring by consumers to safeguard themselves against identity theft render current efforts to combat identity theft ineffective without stronger identity theft laws. Graves et al. further contend that monitoring costs are inequitably burdensome for vulnerable population groups such as our elderly and poor. Using examples in a cost benefit analysis thought process, Graves et al. imply that without accountability (via prosecution and consequences), identity theft represents criminal opportunities with a disproportionate lower risk to the bad actor. Simply put, most identity thieves suffer little to no consequences in the current social and legal environment of the United States. Graves et al. conclude that prevention and victim recovery costs for identity theft need to be reduced, and that incidents of identity theft may themselves be reduced through a policy of harsher sanctions as a deterrent to would-be bad actors.

An analysis of the research data in this literature review demonstrates that identity theft inflicts harm upon individuals, businesses, and commerce. The evidence suggests that despite current efforts of government and law enforcement agencies as well as private sector businesses, reported numbers of identity theft incidents are increasing dramatically.

***Therefore, there is a need for a program to combat identity theft and safeguard our citizens, businesses, and government institutions***

Literature review regarding evaluations of identity theft programs and their effectiveness found little or no substantial information, despite a great deal of literature and studies being conducted on the topic of identity theft itself. Such programs would involve activities such as enforcement and prosecution, public education and outreach, as well as victim assistance programs provided by government institutions or private-sector entities (e.g., businesses or non-profit advocate groups).

Green, Gies, Bobnis, Piquero, N. L., Piquero, A. R., & Velasquez (2020) assert that while there is a great amount of existing literature regarding identity theft itself, there is not a lot of literature exploring crime victim services specifically targeting victims of identity theft. Green et al. uses data obtained via interviews of identity theft victims as the basis of their study to add to the pre-existing literature on the topic, as well as to develop recommendations on how currently existing crime victim services designed to facilitate recovery for identity theft victims could be improved. Green et al. addresses the anxiety and fear identity theft victims experience as being similar to those of sexual assault victims, in that in each type of crime victim, the person has a fear of not being believed by law enforcement or by other institutions. Green et al. further indicates in its findings that victims of identity theft reported geographical considerations as being barriers in the ability of crime victims to obtain services to recover from the crime. Such

geographical considerations also impact the ability of advocates and law enforcement to hold identity thieves accountable. In their reviews of law enforcement, government, and crime victim services provided by other advocates and sources, Green et al. stress the importance of any such service provider clearly communicating that recovery from identity theft relies on the persistence of the victim, and may take a substantial amount of time. Green et al. concludes that each component in the process (e.g., law enforcement, government agencies, advocate services, businesses, etc.) has a different role to play in the recovery of a victim of identity theft.

Drew & Farrell (2018) indicate that cybercrimes and forms of identity theft continue to increase “exponentially” in Australia, and that historical policing methods used by law enforcement in handling other types of crime are obsolete and ineffective when dealing with cybercrime, especially in consideration of the increasing inventiveness of schemes and perpetrators more often than not being located outside of the geographical area of a given jurisdiction. Drew et al. suggest strategies to prevent and minimize risk of identity theft as being an effective tool in combatting identity theft and cybercrime. Drew et al. make suggestions for prevention programs led by law-enforcement regarding cybercrime and online fraud, and imply a premise that prevention is a methodology where police agencies can make effective use of available resources to reduce cybercrime.

On the federal level, the Federal Trade Commission (“FTC”) provides a substantial amount of literature about identity theft including victim support strategies accessible via website (Retrieved February 12, 2022). On the state level for Wisconsin, the Wisconsin Department of Agriculture, Trade & Consumer Protection (“DATCP”) also provides substantial literature about identity theft and victim recovery accessible via website for the Wisconsin public.

In conclusion, literature review on the topic of identity theft and cybercrime suggests that

an effective multifaceted systematic approach for combatting identity theft would include substantial education and outreach efforts as well as a combination of prevention & deterrence efforts, victim recovery services, and enforcement efforts that involve investigation, litigation, and prosecution efforts. Although state agencies such as the Wisconsin DATCP and federal agencies such as the FTC employ a combination of prevention and victim recovery strategies to combat identity theft and to assist identity theft victims, neither of these programs involve efforts or detailed strategies to conduct substantive investigation and criminal prosecution. In Wisconsin, local law enforcement agencies adopt the same strategies as DATCP, or refer crime victims to that agency as well as the FTC for victim assistance. Literature reviews suggest that there is currently a void for the common use of enforcement (investigation, litigation, and prosecution) as an equally valuable part of a strategy to deter, prevent, reduce, or otherwise address identity theft.

### **III. Theoretical Framework**

Both the social contract theory and the social control theory can be applied to occurrences of identity theft and society's collective responsibility and obligation to make reasonable efforts to deter, prevent, detect, and investigate incidents of identity theft and to ultimately hold perpetrators of these crimes accountable through prosecution efforts. These theories collectively explain the need for maintaining control over the social order of society in order to be effective in providing protections and benefits to the population, and argue that a society's formalized institutions are morally obligated to do so.

#### **Social Contract Theory**

At its most basic, the Social Contract Theory is simply a premise that individuals assemble to form a collective society for mutual aid and benefit. Seabright, Stieglitz, & Van der

Straeten (2021) contend that early influential political philosophies such as those of Hobbes, Locke and Rousseau underestimated the complex nature of human behaviors, social relationships, and morays as they relate to the formation and functioning of smaller societies that do not possess strong institutionalized forms to implement social controls. Through a focus on five (5) areas for human motivation, Sebright, et al. posit that earlier views regarding social contracts, their development, and the enforcement of such arrangements may have been different had the totality of human motivations been considered. Sebright, et al., define those five areas as follows:

“(1) what motivates human beings; (2) what constraints our natural and social environments impose upon us; (3) what kind of society emerges as a result; (4) what constitutes a fulfilling life; and (5) what collective solutions can improve the outcome.”

Sebright, et al., applies these five areas in their study of what they term “small scale” societies, and conclude that such societies can achieve great benefits for its members while lacking formalized institutions to provide them. However, Sebright, et al., indicate that the application of the concept of a social contract is valuable in defining the collective society’s expectations of its political institutions.

The study of Sebright, et al., suggests that as humans are social creatures, humans develop forms of both formal and informal rules that govern the behaviors of a collective’s participants. However, the study also implies that larger societies exist under a form of social contract, wherein participants have given up individual independence in favor of the benefits that being a member in a collective society provides for its participants (e.g., safety and security).

According to an early work of Buchanan (1977) exploring the social contract theory, individuals must agree or achieve a consensus to live in a society, and such agreements

define both the rights of society's members and the limitations on personal freedoms and definitions of prohibited conduct.

Modern societies are socially complex, being essentially a conglomeration of groups of individuals, government institutions, and businesses, each possessing further subcultures and subgroups of their own. Donaldson & Dunfee (1994) explore concepts of business ethics and present the Integrative Social Contracts Theory ("ISCT"), which creates a multi-level social contract system for businesses intended for decision-making processes that combine an awareness of social issues and local cultural norms. Donaldson, et al., indicate that the model is applicable to a variety of ethical issues faced in commerce, such as environmental impact considerations, impact on local economies, impact of corporate takeovers and buyouts, the treatment of employees, and the obligations of being a good corporate citizen. Baird & Mayer (2021) provide a focus on ISCT and implications to divisive political and social issues currently being experienced within the United States. Baird, et al., uses gun control in the United States as one such controversial topic where the population is not only divided, but so are American corporate interests. While increases to stricter controls are intended to provide benefits and increase safety for society as a whole, organizations such as the National Rifle Association ("NRA") and other lobbyists fight against such measures in the interest of maintaining or increasing the profits of gun manufacturers. Arguably, a parallel circumstance is created by the conflicting nature between corporate interests and increased efforts to combat identity theft that may restrict commerce. Competing interests create barriers to fulfilling the expectations of a social contract for all of a given collective population.

Buchanan & Musgrave (1999) later expand the social contract theory by providing two differing views regarding the role of government in the context of financial markets, as

Buchanan argues for limiting government interference, citing flaws in political and legislative processes, while Musgrave argues for government policies to correct failures in financial markets and inequities within society. This work demonstrates that governments must strike a careful balance between the two positions to best meet the societal expectations of the social contract.

Both competing corporate interests and dramatic differences in moral beliefs between societal members can be problematic regarding the fulfillment of the expectations of the social contract. Moehler (2018) indicates that moral diversity presents barriers or challenges to multi-level social contracts and stability within society, and explores the difficulties of bringing together a population into one societal collective when its individuals possess differing moral beliefs and practice varying standards of personal conduct.

In his work, Caton (2020) aligns the social contract theory of Buchanan with the concepts of multi-level social contracts of Moehler, especially in regard to concepts of moral order and the moral community of Buchanan. Caton addresses the combination of the works of Moehler and Buchanan as presenting the social contract as forming the basis of establishing behavioral norms for members and the social construct for conflict/dispute resolution between community members. Caton indicates that in more sophisticated societal order (e.g., multi-level or possessing multiple institutions of control), the established multi-faceted systems tend to promote experimentation and ongoing evolution of the community's/society's sense of moral order. Caton implies that a society may adapt its established sense of moral order to changes in the context of the environment in which the community or society exists and operates.

Inusah & Gawu (2021) argue that the obligations of corporations to act morally isn't the product of a social contract, but rather that their moral obligations are supported by the social contract of society. Inusah, et al., contends that the social contract doesn't impose moral

obligations upon the corporation, but the existence of the social contract and the expectations of its society's members explains how corporations develop moral obligations regarding the communities in which they operate.

By extension, under the understanding and definitions of the Social Contract, institutions of a society have an obligation to protect societal members from the harm of identity theft and simultaneously prohibit individuals from engaging in the harmful activities that are defined as forms of identity theft. These aligned outcomes can be theoretically achieved through various forms of social control exerted by society's institutions (e.g., formalized governments, organizations, and businesses).

### **Social Control Theory**

The Social Control Theory of Hirschi (1969) posits that criminal behavior requires some form of motivation to incite antisocial behaviors and criminal misconduct, and that social ties such as family, friends, social circles, schools, the workplace, or other similar constructs of a society reduce the likelihood for people to engage in such antisocial or destructive behaviors. Hirschi further contends that when such social bonds are not established or weak for a person, he or she is more likely to act out with antisocial, deviant, or criminal behavior.

Hirshi's themes on social control are applicable to our society's handling of identity theft matters in two ways: first, increasing the likelihood of individuals not committing identity theft in consideration of societal bonds, the knowledge of the harm inflicted upon others both directly and indirectly as a result of identity theft, and empathy for others, as Hirschi posits that societal considerations are a meaningful deterrent; and second, the obligations of individual members of our institutions to act regarding resolution (e.g., victim assistance, restoration of losses, etc.) and enforcement (e.g., investigation, prosecution, etc.).

While identity theft has only been codified federally as crime since 1998 (Federal Trade Commission, Retrieved February 12, 2022), followed by similar actions by states, actions now defined as identity theft have occurred throughout history, and other criminal violations also potentially apply to the activities. However, the increased use of cyber and internet technologies have exposed users to increased risks, as current identity theft events generally involve some element of cybercrime or online activity. Cheng (2021) contends that the premise of Social Control theory is related to policing and regulation in relation to crime and socially deviant behaviors. Cheng explores social control in the context of modern society and the use of online and social media, which has increased the spread of disinformation. Online activity and social media use also provide opportunities for nefarious actors to obtain identifying information of users.

Internet users and potential bad actors online seem less influenced by societal factors of social control in comparison to direct in-person activities. Ellonen, Minkkinen, Kaakinen, Suonpää, Miller, & Oksanen (2020) conducted a study using a sampling of juveniles from Finland, and comparing online and offline self-control and delinquency in the general context of the social control theory and the effects of varying levels of parental influence on delinquency. The findings of Ellonen, et al., indicate that parental presence, support and control impacted the conduct of juveniles offline, while such parental control had a decreased influence on delinquency occurring online.

A complex society's economy is dependent upon the success of its commerce and businesses, and their role concerning forms of social control within society. The value attributed to specific markets are dependent upon their impact on the community or society (Guizzo & Vigo de Lima 2017). Commerce and business success is threatened or reduced with identity theft

and fraud events. Logically, industries and businesses seek to obtain profits via providing benefits to consumers (societal members) while minimizing risks or harms, if not out of a sense of moral obligation, then out of self-interest and the ability to prompt consumer transactions, etc. Economics and commerce further impact how a nation's institutions provide regulation and oversight, and the levels of care and protection that are provided (Guizzo & Vigo de Lima 2017).

Cingano & Tonello (2020) explore social control and the cause/effect relationships between improved law enforcement and dismissals of Italian local units of government suspected of being infiltrated by organized crime, and the effects such dismissals have on Italian local crime rates. Cingano, et al., indicate that corrupted units of government represent a breakdown of social control, and found that removal of corrupt units of government appeared to result in a ten percent (10%) reduction in minor crimes for the associated community.

Ren, Zhao & He (2019) explore the Broken Windows theory as it relates to social control and the levels of community member participation in crime prevention efforts, and found that deficient or a lack of social controls within a community result in a reduced support and participation of individual citizen community members in the crime prevention efforts of the local institutions. The Broken Windows theory posits that community members perceiving disorder and a lack of social controls (i.e., policing or regulatory oversight) experience a greater fear of crime victimization, and as a result, these community members are less likely to contribute to crime prevention efforts of the community. In such circumstances, citizens believe that the efforts are useless in impacting crime and put their safety at risk, and that such risk is not reasonable in their individual cost benefit analysis.

Both the Social Contract and Social Control theories are applicable to identity theft, fraud, and cybercrimes within the United States. Social Contract applies to how we as a

collective society address these crimes, the expectations of our society's members to be protected from such harm and the obligations of our institutions to act (e.g., mutual aid, benefit, safety and protection, etc.). A failure to effectively act represents at its most basic a threat to the fabric of our social order and the motivation for individuals to remain as contributing participants in a collective society. The Social Control theory applies not only to the premise of collective society acting to provide protections for its individual members, but also enforcement actions taken to hold bad actors accountable. Without accountability, bad actors will continue to perpetrate the crimes of identity theft, and as indicated by current trends, the crime rates escalate. Such escalation and the resulting victimization could arguably weaken societal bonds of individuals for collective society as a whole.

#### **IV. Program Evaluation: Current Practices for Identity Theft Enforcement efforts and/or Prevention and Education/Outreach Programs**

Numerous levels of government agencies and private-sector advocates exist to address identity theft matters For Wisconsin residents. However, while both private-sector and public-sector sources in existence that provide valuable services and support to members of the general public regarding identity theft, there are few if any programs that specifically target identity theft and aggressively integrate investigation and enforcement into other prevention and recovery approaches, within either the State of Wisconsin (DATCP website, Retrieved February 12, 2022) or the whole of the United States (FTC website, Retrieved February 12, 2022). Nonetheless, various government programs and private-sector advocates provide valuable public education for citizens to safeguard their information, minimize risk, and prevent identity theft as well as assist victims in recovering from identity theft when victimization occurs.

Local Law Enforcement – Wisconsin law obligates local law enforcement agencies to take reports of criminal identity theft and bases jurisdiction for ID theft matters upon the residence of the victim (Wisconsin Legislature website containing criminal statutes, Retrieved February 12, 2022). Like many cities throughout the country, the City of Madison, Wisconsin Police Department uses a citizen self-reporting system for multiple types of property crimes, including identity theft (Madison Police website, Retrieved March 22, 2022). In addition to taking citizen reports, most local law enforcement agencies also provide complainants fact sheets and contact information for other agencies to assist them in victim recovery efforts. These self-help efforts are therefore dependent upon the follow-up actions of the complainant/victim regarding his or her own recovery.

Federal Trade Commission – The programs of the FTC are often used as a model for other states, and provides a substantial amount of information for other agencies to use, as well as fact sheets and information for individual citizens. That information focuses on the prevention of identity theft as well as victim recovery (FTC website, Retrieved February 12, 2022).

State of Wisconsin – When considering state government agencies, the primary program to combat identity theft in Wisconsin is housed within the Department of Agriculture, Trade & Consumer Protection (“DATCP”) (DATCP website, Retrieved February 12, 2022). DATCP partners with other state agencies as well, and collaborates to both educate the general public as well as provide complaining victims with victim support and recovery efforts. For example, the Wisconsin Department of Justice website has a public page which links directly to the DATCP PDF file of an identity theft complaint form (WI DOJ website, Retrieved March 22, 2022). Although the website contents and program are similar in design to the identity theft program(s)

of the Federal Trade Commission (FTC), DATCP identity theft program staff are able to interact with citizen complainants throughout its processes. This differs from some self-reporting mechanisms of the FTC or even some local law enforcement agencies, where the citizen receives little or no direct follow-up after filing their initial complaint information.

### **Current Law Enforcement Practices in Wisconsin for Handling of ID Theft Complaints**

Wisconsin law enforcement agencies employ policies regarding the handling of identity theft complaints in compliance with statutory reporting obligations, and provide complainants with the law enforcement agency case number for the complaint filed. Law enforcement agencies may further provide limited victim assistance via supplying fact sheets and other contact information to other agencies for victim recovery services. However, based on reviewing the practices and websites of the Madison Police Department (“MPD”) and the Wisconsin Dane County Sheriff’s Department (“DCSD”), little follow-up is offered in general. According to annual reports and its website (Retrieved March 24, 2022), the DCSD provides little information specific to identity theft matters, with the DCSD 2009 annual report addressing identity theft within the context of statistics, computer forensic investigation assignments, and collaborations with Madison Police Detectives, while the 2019 annual report for DCSD only briefly addresses general fraud and in the context of training provided by DCSD to a smaller suburban police department.

As indicated by the United States Department of Justice (“USDOJ”) regarding community policing projects and the need for multi-agency collaborations and a national strategy to combat identity theft, both historic and current law enforcement investigations and criminal prosecutions specific to identity theft occur infrequently, and when such enforcement activities do occur, they typically involve circumstances in which identity theft activities are part of a

larger fraud scheme (Cops office: Grants and Resources for Community Policing. (n.d). Retrieved March 26, 2022).

### **Current Methods and Strategies Employed by Government Agencies**

The current programs administered both federally as well as on the state level regarding identity theft involve a focus on prevention via outreach efforts and victim recovery assistance. Although agencies provide duplicative information, each agency targets their own citizen group populations. For example, the federal Office of Justice Programs, Office for Victims of Crime provides a *Statement of rights for identity theft victims* accessible via website (Retrieved March 24, 2022), which in part advises victims of both their rights to placing fraud alerts and credit freezes on their information as well as contact information for credit reporting agencies to do so. DATCP (DATCP website, Retrieved February 12, 2022) provides the same information.

### **Current Strategies Employed by Private-Sector Businesses**

Wisconsin Law Enforcement agencies are statutorily obligated to take a citizen complaint or report concerning identity theft, and most private-sector businesses and financial institutions make filing a police report a requirement as part of their internal processes when resolving matters that involve fraudulent transactions via identity theft. Private-sector businesses as well as public-sector organizations also have legal obligations regarding data breaches and informing those individuals who have had their personally identifying information compromised (Bisogni, et. al, 2020), which can incur considerable costs for those entities. As such, entities have both legal and financial motivations to safeguard personally identifying information and avoid such costs (Romanosky, et. al, 2011).

Business strategies to combat identity theft are primarily focused on prevention (Shah, Maitlo, Jones, & Yusuf. 2019) and mitigation of losses for the business itself (Payne, et. al.

2017). However, private-sector businesses are also motivated to maintain the confidence of their consumer base and promote continuing transactions with their business, especially those involving online commerce (Hille, et, al, 2015).

### ***Enforcement vs. Business Practices***

For matters of identity theft within the jurisdiction of Wisconsin, law enforcement agencies are initially concerned with meeting the statutory obligation of taking a report, while businesses are initially concerned with their legal obligations under the Fair Credit Reporting Act (“FACTA”) (*Fair credit reporting act*. Federal Trade Commission. Retrieved March 24, 2022) and other legislation. Under the umbrella of FACTA, victims of identity theft have legal protections against businesses attempting to collect payment on fraudulent transactions, reporting on fraudulent accounts/transactions to credit reporting agencies, and businesses are obligated to cease any collections activities. Additionally, businesses are obligated to provide transaction records to the victim when requested.

### ***How Fear of ID Theft Impacts Commerce***

Online commerce is substantially impacted by consumer perceptions of the internet medium in relation to consumer perceptions of the risk of identity and financial information being compromised via online purchase transactions and the potential for becoming a victim of cybercrime (Apau, et. al, 2019). Consumers may have negative associations with online platforms, hesitating to buy products online resulting from fear of identifying information being subsequently compromised (Hille, et. al, 2015). Businesses must successfully create a balance between operational controls/safeguards regarding technologies used for commerce via electronic purchase transactions and the convenience for the end user and business performance, which is typically measured by profits generated by sales transactions (Shareef, et. al, 2019).

***Taxes, Capital Loss Claims, Reduced Operating Revenue for Government***

Both businesses and government agencies have benefitted from advances in products, electronic communications, and internet technologies, but these same technologies have also provided increased opportunities for the commission of identity theft and tax crimes (Leighton, 2019). Imposters earn income and avoid paying the associated income taxes by passing the tax obligations on to their victims, which causes loss of tax revenue when victims are relieved of the tax burden once evidence of identity theft has been established (Leighton, 2019).

Regulatory oversight of business practices, such as safeguards against fraud and enforcement of tax rules, have been found to improve overall business performance (Mironov 2013). For example, Russian firms subjected to strict tax enforcement performed better than Russian firms diverting funds, etc. as part of their practices (Mironov 2013). In the United States, the federal Internal Revenue Service (“IRS”) has begun collaborating with State authorities and private sector tax preparation businesses to curb identity theft, which resulted in a 46% decrease in reported tax-related identity thefts between 2015 (about 699,000) and 2016 (about 376,000) (Cohn, Michael 2017).

**ID Theft Victims (General, Youth, and Elderly)**

Statistics from the FBI’s Internet Crime Complaint Center (“IC3”) demonstrate that victims of identity theft are from all age groups, (Internet Crime Report 2020), and further suggest that anyone can become a victim of identity theft and that victims of reported identity theft come from all walks of life.

Children have their personally identifying information stolen by imposters not only to fraudulently obtain goods/services, but potentially to establish credit, to avoid legal process, or otherwise escape any stigma associated with their own identity (Navarro, et. al. 2016).

Elderly adults are targeted by fraudsters in part because they are generally more trusting and polite than younger adults (Elder fraud. FBI. Retrieved March 26, 2022). The National Institute on Aging indicates that elderly victims of financial exploitation typically suffer not only the initial financial losses while being on a fixed income, but also cascading effects that cause additional harm, such as worsening medical conditions or in more severe instances, premature death (*Elder abuse*. National Institute on Aging. Retrieved March 26, 2022). According to the IC3 2020 Elder Fraud Report (Retrieved March 26, 2022), elderly victims are typically targeted by identity thieves so that they obtain personally identifying information to act as imposters to either access and drain funds from pre-existing financial accounts or to establish new lines of credit accounts. The report also indicates that fraudulent activities impacting elders also include imposters posing as government officials to gain the victim's trust and access to personally identifying and financial information, or access to financial accounts.

As indicated by both the FTC (FTC website, Retrieved February 12, 2022) and DATCP (DATCP website, Retrieved February 12, 2022), one of the differences between adult and underage identity theft victims is that until the minor turns 18 years of age, their being victim of identity theft may have gone undiscovered until that time. In such instances, the identity theft is often discovered when the young adult applies for lines of credit, loans, or sources of college funding, where the circumstances may impede the young adult's ability to obtain employment, rent housing, or attend a college (Navarro, et. al. 2016). In contrast to this, an imposter victimizing an elderly victim impacts the elder's ability to pay basic costs of living, housing, and medical care, as they are commonly dependent upon a fixed income from being a retiree (*Elder abuse*. National Institute on Aging. Retrieved March 26, 2022).

The study of Green, et. al, (2020) indicates that identity theft victims may struggle through recovery from identity theft and related fraud, and will experience barriers to taking the appropriate steps in making themselves whole. Victim service programs are beneficial to identity theft victims in being able to successfully navigate through the steps of recovery as well as communicate with businesses and financial institutions involved in their identity theft matter (Green, et. al, 2020).

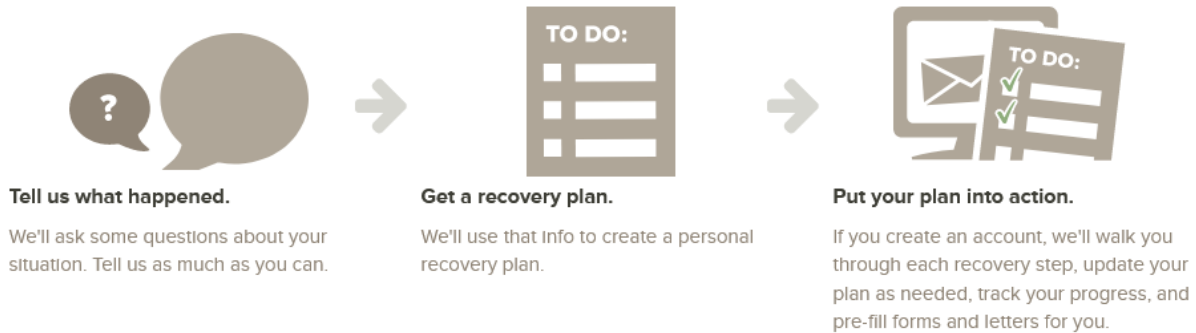
### **Current State – Prevalent Programs**

The services available to the Wisconsin public via identity theft programs essentially stem from a loose collaboration between law enforcement agencies and recovery programs: Law enforcement takes criminal complaints and provides the complainant an associated case report number. Some victims discover the programs independently, and law enforcement frequently refers victims to state or federal ID Theft programs or private sector advocates that provide recovery services. Victims are typically directed via program assistance to follow-up with credit reporting bureaus as well as the businesses and financial institutions involved with the ID Theft activities to both prevent additional or continuing victimization (e.g., fraudulent establishment of new accounts, ongoing billing by businesses, collections activities, etc.) as well as to recover from the effects of identity theft (e.g., correct credit reports, close fraudulent accounts, correct medical or tax records, etc.). Presently, the process concludes once the victim has recovered from the crime.

The FTC provides public access to its identity theft program via a website (*Identitytheft.gov*. Retrieved March 26, 2022) that presents an overview of its general processes as follows:

IdentityTheft.gov can help you report and recover from identity theft.

**HERE'S HOW IT WORKS:**



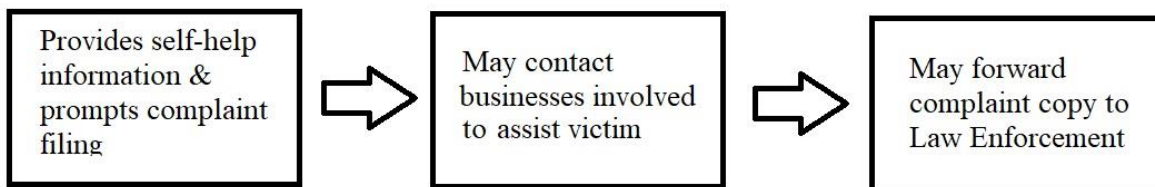
[Get started now.](#) Or you can [browse a complete list of possible recovery steps.](#)

Graphic from FTC website [www.Identitytheft.gov](http://www.Identitytheft.gov). Retrieved March 26, 2022

In addition to victim recovery services, the FTC also promotes strong prevention strategies via education and outreach efforts.

As the most prevalent identity theft program for Wisconsin citizens is administered by DATCP and mirrors its federal counterpart, a brief overview of the program’s victim assistance services (DATCP website. *Identity Theft Protection*. Retrieved February 12, 2022) is as follows:

**Overview of Victim Assistance Provided by Wisconsin Consumer Protection**



Like the FTC program, the DATCP processes for assisting identity theft victims not only offer recovery support, but also includes substantial public education and outreach efforts for the purposes of preventing identity theft.

Neither the FTC nor the DATCP provide direct statistical data regarding arrests and/or prosecutions for identity theft for specific jurisdictions or in general.

There is a lack of directly comparable data from government sources to determine the relationship between identity theft reports and identity theft prosecutions. This author conducted searches of multiple publicly accessible sources of information including: identity theft reports from the FTC ([www.ftc.gov](http://www.ftc.gov). Retrieved March 26, 2022); crime statistics from the Uniform Crime Reporting (“UCR”) Program (Retrieved March 26, 2022); prosecutions involving general property crimes (<https://measuresforjustice.org>. Retrieved March 26, 2022) and Dane County, Wisconsin Court filings (from <https://courts.countyofdane.com/Court/Cases>. Retrieved March 26, 2022); and Dane County, Wisconsin Population data (U.S. Census Bureau. Retrieved March 26, 2022). Data from these sources has been incorporated into *Table 3* below.

**Table 3: Reported ID Theft to FTC vs. UCR Arrest Data for Fraud Categories**

Year	Wisconsin Population per US Census Bureau	Wisconsin ID Theft Reports per FTC (Approximate*)	Wisconsin Arrests per UCR ID Theft Related Fraud	Dane County Population per US Census Bureau	Dane County Arrests per UCR ID Theft Related Fraud	Dane County felony prosecution cases per DCCS
2019	5,837,985	5,020	27,915	546,695	293	3,128
2020	5,893,718	9,076	23,357	551,442	189	3,269
2021	5,895,908	11,379	unavailable	556,189	unavailable	unavailable

*\*Calculations based on X number of reports per 100K population*

According to the data for Wisconsin from the FTC Consumer Sentinel (Retrieved March 26, 2022), there were: 193 reports of identity theft per 100,000 population for the year 2021; 154 reports of identity theft per 100,000 population for the year 2020; and 86 reports of identity theft per 100,000 population for the year 2019, demonstrating a significant increase in identity theft reported to the FTC.

UCR Arrest Data obtained from the Wisconsin Department of Justice (Retrieved March 26, 2022) indicates the following when limited to the property crimes of Forgery & Counterfeiting, Fraud, and Embezzlement, all of which would include identity theft and related crimes: 189 arrests for the year 2020 for Dane County, and 23,357 total arrests for Wisconsin; and 293 arrests

for the year 2019 for Dane County, and 27,915 total arrests for Wisconsin. According to Dane County Court filing statistics (Retrieved March 26, 2022), there were 3,269 felony prosecution case filings for the year 2020 and 3,128 felony case filings in the year 2019. The UCR reporting mediums make use of broad crime categories that are not specific to identity theft, and Dane County data differentiates between felony and misdemeanor, but is not otherwise offense specific.

As detailed previously under the literature review for this research paper, while the FBI UCR categories are not specific to identity theft, the FBI's IC3 does report complaint filing data regarding cybercrimes that are specific forms of identity theft (e.g., Credit Card Fraud; Loan or Lease; Bank Fraud; Phone or Utilities; Employment or Tax-related; Government documents or benefits; and Other) and estimated dollar losses attributed to identity theft incidents. It does not provide specific data for IC3 complaint filings regarding investigative follow-up, prosecutions, or case disposition.

It has not been possible to obtain publicly accessible data to accurately determine the relationships of reported identity theft and levels of follow up investigation and prosecution referrals. However, the publication *Cybercrime & Identity Theft Statistics 2021: Policy Advice* (Kopestinsky, 2022) for the insurance industry estimated, based on 2006 research, that only 0.14% of identity theft suspects were arrested in federal cases, which at that time equated to one (1) in seven hundred (700) identity theft suspects being arrested. This information suggests that follow-up actions by law enforcement such as detailed identity theft investigations and subsequent arrests of identity theft suspects don't regularly occur. This translates to fewer prosecution referrals for identity theft. According to the federal Office for Victims of Crime,

only 1 out of 10 identity theft victims filed reports with the police in 2012 (Office for Victims of Crime 2016).

### **Cause and Effect: Social Harms Inflicted from ID Theft Crimes**

Fraud schemes and identity theft causes various levels of harm. According to White-Collar Crime information (May 3, 2016) from the United States Department of Justice website Retrieved March 24, 2022), victims also suffer psychological harms and feelings of betrayal trust in addition to any financial losses.

Identity theft victims often suffer both emotional and physical effects which includes depression and poor health (Golladay & Holtfreter, 2016). People report having felt anger, betrayal, helplessness, shame, and a sense of loss after becoming an identity theft victim (Golladay, et. al, 2016). Additionally, those reactions also expand into a loss of consumer confidence by identity theft victims, making them hesitant or unwilling to make purchase transactions or investments (Golladay, et. al, 2016).

In many incidents of identity theft, the bad actors are related to the victim in some way, (e.g., family members, friends, or friendly acquaintances) as opposed to a complete stranger, especially when ID theft victims are children (Betz-Hamilton 2020). With instances of familiar fraud, more often than not, the bad actor has known the victim in some way for years, or may have social ties to victim via a few degrees of relational separation (i.e., a friend of a friend, etc.) and the crimes destroy interpersonal relationships through victimization and a sense of betrayal (Golladay, et. al, 2016). The emotional harm of fraud on people influences a person's sense of judgment and decision-making processes (Golladay, et. al, 2016), which by extension influences their future financial transactions, online purchases, etc. (Shareef, et. al, 2019).

In addition to any direct losses suffered by businesses due to identity theft related fraud, reduced consumer confidence results in lower sales and loss of sales revenue for the business (Kumar & Shareef, 2012). Businesses also suffer losses associated with the costs of a data breach, which can occur either by the business having been targeted by cybercriminals or forms of cyber intrusion, or via accident or carelessness of the business itself (Bisogni, et. al, 2020). Costs to mitigate the effects of a data breach can be significant, and likely include the expenses of corrective action (security software/product costs and labor costs) and potentially the added expense of credit monitoring services that would be offered to the business' clients/customers impacted by the breach (Bisogni, et. al, 2020) or potential legal liability as a result of a data breach (Yenouskas, et. al, 2018).

Current prevalent programs provide valuable services to the public. However, as implied by Braga, et al. (2019) regarding the policing of disorder, a failure to thoroughly investigate identity theft crimes, a failure to both identify and arrest bad actors, and a failure to prosecute identity thieves fails to deter crime/promotes crime, which inflicts harm upon the social order. Although the online publication *Five things about deterrence* from the National Institute of Justice (Retrieved March 27, 2022) indicates that harsh sentencing does little for deterrence, it also posits that the perception of being caught and being held accountable is a strong deterrent, and by extension suggests that a lack of such consequences for criminal behaviors creates an environment that promotes crime.

#### **IV. Recommendations**

Recommendations for a model government program to combat identity theft and its ideal components are predicated upon findings from evaluations of current and pre-existing programs, literature review, and the theoretical framework explored within the scope of this research paper.

Based on the research of this paper, program target areas have been identified for consideration in the development and implementation of a model identity theft program useful for government entities for the purpose of combatting identity theft and protecting the public.

### **Presentation of Statistical Evidence for Better Understanding of the Problem**

Based on the research of this paper, the lack of publicly available and accessible statistics for incident tracking of investigations, arrests, outcomes, and case dispositions specific to identity theft and identity-theft related crimes (e.g., credit card fraud, forgery, etc.) by law enforcement and government agencies throughout the United States is problematic for understanding the true scope of identity theft and its impact on our society.

Identity theft data from the Wisconsin Office of Privacy Protection for the years 2007, 2008, and 2009 demonstrates that people reporting identity theft victimization to the FTC failed to also file police reports at the rates of: 65% did not notify police in 2007; 65% did not notify police in 2008; and 28% did not notify police in 2009 (Wayback Machine, n.d., webpage captures for “wi.privacy.gov”). While this FTC data indicates increased reporting to police between 2009 and previous years, these statistics are limited to those that filed reports with the FTC and not a true representation of identity theft victims overall within the United States. The federal Office for Victims of Crime indicates that 10% of known identity theft victims filed police reports in 2012 (Office for Victims of Crime, 2016).

Identity Theft data regarding reports, arrests, prosecutions, dispositions and outcomes should be collected and maintained for public access in a manner consistent with how the Wisconsin Department of Justice (“WI DOJ”) currently collects and maintains Domestic Abuse data (WI DOJ, 2019, Domestic Abuse Data section). This data is easily accessible via its website. WI DOJ mandates reporting for all domestic abuse incidents by law enforcement and

prosecutor's offices, which includes arrests, prosecution charges issued, and case dispositions. WI DOJ derives their statistics on domestic abuse from such reporting. Reports from law enforcement agencies and prosecutor's offices include a wide variety of statutory offenses attributed to incidents, but then further indicate that the incident was attributed to a domestic abuse incident or statutory domestic abuse enhancers may be included (WI DOJ, 2019, Domestic Abuse Data section). Considering this current reporting program of WI DOJ, a reporting program for identity theft could be created that mirrors Wisconsin's current domestic abuse incident tracking program. Such a reporting mechanism would provide accurate data regarding the scope of identity theft and nature of identity theft incidents that would be useful for programmatic decisions.

Reporting systems need to be established and maintained for obtaining accurate data regarding identity theft incidents and dispositions. Such information is important to make the best possible data-driven decision regarding program creation, implementation of program efforts and strategies, programmatic adjustments and changes, and for determining the impact of identity theft programs via monitoring and use of such specific and relevant data.

### **Ideal Components for Program Overview**

According to the Identity Theft sections of their respective websites, the prominent and current identity theft programs of the FTC (Retrieved March 26, 2022) and DATCP (Retrieved February 12, 2022) provide services to the public through a combination of education, prevention, and victim recovery efforts and protocols. However, the identity theft programs of the FTC and DATCP lack enforcement efforts that include detailed investigation, resulting arrests and prosecution referrals, and case prosecution efforts in identity theft matters. While the Internet Crime Complaint Center ("IC3") website of the FBI (Retrieved March 26, 2022)

demonstrates that the IC3 takes complaint information for identity theft, according to the FBI website Identity Theft section (Retrieved April 3, 2022), the FBI uses the information and maintains a database regarding cybercrime in general, and refers victims to the FTC for information about recovery from identity theft. In the context of the numbers of complaints submitted and according to the Victim Services section of the FBI website (Retrieved April 4, 2022), the FBI does not typically initiate white collar crime/cybercrime investigations of every individual complaint matter received via the IC3 or otherwise, but rather when circumstances of complaint matters meet criteria set by the internal policies. Wisconsin local law enforcement is legally obligated to take an identity theft report from a complaining witness, but the media and websites of police departments for three large Wisconsin cities suggest that they typically do not conduct detailed investigations, which includes the Identity Theft section of the website for the Milwaukee Police Department (Retrieved April 5, 2022), the Self-Reporting System section of the website for the City of Madison Police (Retrieved March 22, 2022), and the Identity Theft section of the website for the Green Bay Police Department (Retrieved April 5, 2022).

Ideal components within a model program are complementary and include: (1) Prevention and Security; (2) Public Outreach and Education; (3) Victim services and recovery efforts on behalf of victims; and (4) Enforcement efforts. While each of these target areas appear to superficially involve separate efforts and intended outcomes, the activities involved in each target area may be overlapping (e.g., investigative steps may also simultaneously support victim assistance as well as providing a form of education and outreach to businesses involved in an identity theft matter). Each target area independently appears to be intended to produce outcomes of mitigating identity theft, and the efforts involved in each can be combined. Finally, an ideal program would also include monitoring of the impact of its efforts through the use of relevant

and specific data regarding identity theft. Based on this information, data driven decisions could be made for program adjustments for improved effectiveness and change.

### ***Prevention and Security***

As indicated via the Identity Theft Consumer Information section of the FTC website (Retrieved February 12, 2022), prevention and security efforts regarding identity theft include: safe handling of records; best practices that safeguard personally identifying information and records; efforts to physically secure records and documents containing a person's identifying information; efforts to electronically secure digital records and documents containing a person's identifying information; and making use of safeguards and computer security software products.

### ***Public Outreach and Education***

Various pre-existing programs and public media offer education and information regarding prevention and security measures to mitigate or protect against identity theft, including the Better Business Bureau (BBB St. Louis, 2021), the Identity Theft section of the FTC website (Retrieved March 26, 2022), and the Identity Theft Protection section of the DATCP website (Retrieved February 12, 2022). The Identity Theft section of the FTC website (Retrieved March 26, 2022) indicates that public outreach and education efforts serve as a form of prevention, making members of the public aware of potential risks that could compromise their personally identifiable information as well as best practices and methods to mitigate or eliminate such risks.

Both public and private sector entities have a need to educate their employees on security matters pertaining to physical security of sensitive information and records, computer, internet, and records security practices (Payne, et. al., 2017) and (Burnes, et. al, 2020). Entities further enforce policies regarding such security protocols (Bose & Leung, 2019).

***Victim services and recovery efforts for victims***

The Identity Theft section of the FTC website (Retrieved March 26, 2022) indicates that victim assistance and recovery efforts regarding identity theft involve a range of activities intended to educate the victim regarding self-help actions that include: the need to determine the scope of the identity theft involved (e.g., obtain credit reports and review for discrepancies, freeze credit, identify third parties involved in ID theft matter, etc.); filing a police report and obtaining a case number; communications with businesses involved in fraudulent transactions (e.g., retailers, banks, credit card issuers or other account holders, utilities or telecommunications service providers, etc.); and communications with government entities involved (e.g. Internal Revenue Service, Department of Revenue, Social Security Administration, Department of Transportation, local law enforcement, etc.). As indicated by the DATCP website section titled “File a Consumer Complaint” (Retrieved February 12, 2022), consumer protection agencies typically handle other consumer protection complaint matters (e.g., billing issues, telecommunications service issues, home improvement fraud, etc.) by corresponding with businesses to advise them of the complaint. A regulatory or enforcement agency may communicate with businesses involved in fraudulent transactions while assisting identity theft victims in a manner consistent with how consumer protection programs handle other complaint matters, including efforts to resolve/eliminate complainant/victim liability from fraudulent transactions. With this practice, agencies also assist those businesses involved with the fraudulent activities by advising the business of the fraud and providing information regarding potential faults in their processes which the imposter took advantage of to commit identity theft.

***Enforcement efforts***

Enforcement efforts involve investigation and referrals to a prosecuting authority for

consideration of either civil or criminal prosecutorial action. These prosecution efforts are intended to hold offenders accountable, restore a crime victim's losses, produce a public awareness, and potentially act as a form of deterrence.

*Investigation* – The predecessor program for DATCP's current identity theft program, Wisconsin Office of Privacy Protection ("OPP")(Wayback Machine, n.d., webpage captures for "wi.privacy.gov"), previously included investigation components as evidenced by its Mission Statement (Office of Privacy Protection, 2006) that states, in part:

- "To investigate and assist in the prosecution of identity theft and other privacy related laws, and, as necessary and appropriate, coordinate with local, state, and federal law enforcement agencies in the investigation of similar violations"
- "To assist in coordinating activities of local, state, and federal law enforcement agencies regarding identity theft, identity fraud, and other privacy related violations of law"

The website segment titled "Complaints" for the predecessor OPP (Wayback Machine, n.d., webpage captures for "wi.privacy.gov") contains the following verbiage:

"If we believe an identity thief or business may have violated state laws, we may start an investigation. In some situations, we may recommend the case for prosecution to the Department of Justice or a district attorney. However, further action is their decision."

According to the DATCP website Identity Theft Protection section (Retrieved February 12, 2022), these practices are absent from DATCP's current identity theft program, and the agency's investigators no longer conduct detailed investigations of identity theft matters either independently or in partnership with other authorities for the intended outcome of producing prosecution referrals. Rather, the DATCP website Identity Theft Protection section (Retrieved February 12, 2022) indicates that the agency's efforts are focused on a combination of prevention via education/outreach and assisting with victim recovery.

In a model government identity theft program, investigation is a necessary component not only to hold offenders accountable, but also to provide forms of victim assistance (Graves, et. al, 2017). Victim assistance efforts can be combined with preliminary investigative steps in an identity theft matter, such as putting businesses involved on notice of the fraudulent activity while simultaneously attempting to obtain financial records, etc. Publications from Victim-Witness Assistance of the United States Department of Justice suggest that crime victims have a higher likelihood of recovering from losses attributed to financial crimes through such investigative efforts as well as resulting enforcement actions such as prosecution (The United States Department of Justice, 2015). Golladay, et. al (2016) suggest that law enforcement and prosecution efforts instill a sense of restoration for both the identity theft victim and for society as a whole when such offenders are held accountable. Although investigations of identity theft may be potentially costly and difficult due to the complexities of identity theft incidents, investigation is necessary to provide any level of deterrence via outcomes of arrest, prosecution, or other forms of accountability (Graves, et. al, 2017).

Guizzo, et. al (2017) imply that in consideration of the Social Control Theory, levels of social control influence both regulatory oversight and care for the population. Inusah, et. al, (2021) suggests that in consideration of the Social Contract Theory, the business community and by extension the government have moral obligations to maintain the social order and protect the public.

Civil legal action – Identity theft matters include multiple participants that not only include the victim and the imposter, but also a third party or parties from which the imposter has obtained goods/services or something of value from (e.g., financial institutions, retailers, government entities, etc.). In some instances, such third parties may engage in unscrupulous

actions against the identity theft victim, such as refusing to cease billing for fraudulent transactions or refusing to cooperate with the identity theft victim in restoring their identity. Such matters often not only violate provisions of the FACT Act, but potentially Consumer Protection laws such as unfair billing and service subscription practices as indicated by numerous publications accessible via the Consumer Protection Fact Sheets section of the DATCP website (Retrieved April 5, 2022). Violation of consumer protection laws create legal liability for the business (Wisconsin legislature, n.d., Chapter 100).

Under certain circumstances, District Attorneys' offices are able to bring civil actions against violators of state consumer protection laws (Wisconsin Legislative Fiscal Bureau, 2019, Consumer Protection Programs). As indicated by the Public Protection Unit section of its website (Retrieved April 2, 2022), the WI DOJ possesses a Public Protection Unit that takes referrals from other state agencies that allege various violations of consumer protection laws and civilly litigates cases.

The federal Fair Credit Reporting Act 15 U.S.C. § 1681 ("FACTA") governs consumer rights concerning financial transactions (FTC, 2021, Fair Credit Reporting Act). Under the federal FACTA, consumers have protections and rights regarding financial transactions, including protections against unfair or fraudulent billings and transactions and rights to copies of all records attributed to financial transactions/relationships using their personally identifying information. Consumers additionally have the ability to bring a civil action against businesses involved with their identity theft matter who violate the Fact Act.

Government investigators may also make use of the provisions of FACTA when investigating identity theft matters simply by having complainant victims authorize the agency's representatives to act on behalf of the victim when obtaining records under FACTA (Wisconsin

Office of Privacy Protection, 2006, Authorization for Release of Information form). Use of FACTA via this practice is another tool to assist investigators in their work handling identity theft complaint matters in addition to the use of information requests, subpoenas, and search warrants. Records obtained via FACTA may further establish the probable cause needed to obtain criminal subpoenas or search warrants.

*Criminal prosecution* – A method for matters of identity theft to be resolved would potentially involve the criminal prosecution of an imposter once he or she has been identified via investigation and arrested by law enforcement.

According to the websites of the Milwaukee County District Attorney (Retrieved April 5, 2022), the Dane County District Attorney's Office (Retrieved April 5, 2022), the Kenosha County District Attorney (Retrieved April 5, 2022), and the Door County District Attorney (Retrieved April 5, 2022), Wisconsin District Attorneys' offices criminally prosecute violators of the state's criminal statutes. According to the Criminal Litigation Unit section of its website (Retrieved April 2, 2022, the WI DOJ possesses a Criminal Litigation Unit that criminally prosecutes cases in special circumstances, assists local District Attorney's offices, or potentially in cases involving multi-jurisdictional matters. The Victim Services section of the FBI website (Retrieved April 4, 2022) indicates that Offices for federal Attorneys General prosecute identity theft matters that violate the federal identity theft statute and other federal law.

Each state and federal prosecutor's office represents potential agencies which receive prosecution referrals based on criminal investigations from local, state, and federal law enforcement agencies. While the decision to bring a criminal case against an offender/offenders rests within the authority of each office, prosecution decisions can only be made when case information is referred to them or otherwise brought to their attention.

### **Data Breaches & Security Awareness**

Both government agencies and private sector entities have legal obligations regarding data security and data breaches when they occur (Digital Guardian, Inc., 2018).

#### ***Current Legal Obligations and Liability***

Businesses and government entities alike are subject to legal obligations regarding data breaches under federal and state laws (Digital Guardian, Inc., 2018), including consumer notifications when their personally identifying information has been compromised via data breach. Identity theft victims have additional rights to records and the cessation of billing on fraudulent transactions under federal and state laws, including the federal FACT Act. Businesses and organizations have levels of legal culpability as defined by the FACT Act and other federal and state statutes regarding the mishandling of personally identifying information. The FACT Act provides civil remedies regarding both willful noncompliance as well as noncompliance via negligence of the provisions within the FACT Act.

#### ***Suggested Reporting Mechanisms***

As demonstrated by the Data Breaches section of the DATCP website (Retrieved April 3, 2022), current identity theft programs such as those of DATCP obtain and maintain information regarding known data breaches as well as provide listings accessible to the general public. Additionally, the Data Breach Resources section of the FTC website (Retrieved April 3, 2022) indicates that current programs also provide education and assistance to businesses suffering from a data breach.

As part of a model identity theft program, these pre-existing programs could be continued, potentially expanded upon, and extended via collaboration, networking, or partnerships between agencies. Such programmatic efforts help to build partnerships between

regulators/government entities and businesses regarding data breaches and identity theft matters.

### ***Private Sector Partnerships with Regulators***

A model identity theft program should include building and maintaining effective partnerships between government regulators and businesses as part of its prevention and outreach components. Within an established regulatory framework, such public-sector and private-sector partnerships provide services to the general public and are useful in marketplace monitoring for fraudulent trends, etc. (Pongsiri, 2002). As demonstrated by their website contents, the current identity theft programs of the FTC and DATCP already have an established framework for such efforts. These agencies collectively obtain information from businesses involved in data breaches and inform the public of those breaches, as well as provide information to affected businesses regarding their obligations and recovery steps regarding data breaches. Any new model identity theft program or modification of a pre-existing program to incorporate additional components should include or continue the practices of the FTC and DATCP regarding data breaches.

In conclusion, recommendations for the ideal components within a model program include: (1) Prevention and Security; (2) Public Outreach and Education; (3) Victim services and recovery efforts on behalf of victims; and (4) Enforcement efforts. Each of these areas are complementary in practice, and further involve efforts to both obtain and communicate relevant detailed identity theft data as well as efforts involving data breaches.

## **IV. Conclusion**

The United States has been suffering a consistent increase in identity theft incidents over the past several years. According to the annual reports of the Internet Crime Complaint Center (“IC3”) of the FBI (Retrieved March 26, 2022), the number of complaint filings for identity theft

incidents between 2016 and 2020 have increased approximately 265%, and the reported dollar losses have increased about 280%. Although there is a lack of organized data for identity theft incidents in general, the IC3 reporting data reflects a trend that is harmful to both the institutions and individual members of American society. The insurance industry has estimated that only one (1) in seven hundred (700) identity theft suspects are arrested (based on 2006 data of federal cases) (Kopestinsky, 2022).

Through an exhaustive literature review, it can be determined that while identity theft incidents have been increasing in the United States, the attributed financial losses have also been increasing (IC3, Retrieved March 26, 2022, Annual Reports). Identity theft victims experience many other collateral financial and psychological harms in addition to the initial and direct financial losses suffered from victimization (Golladay, et. al, 2016). The value of a model identity theft program incorporating the recommended ideal components and the impact on victim assistance as well as the potential reduction and prevention of identity theft via deterrence can be understood when applying Hirschi's (1969) social control theory, in that a person's ties/bonds to society curb/deter deviant behaviors. In an extension of the concepts of social control theory, Braga, et. al, (2019) assert that the policing of disorder via less aggressive options of problem-solving practices and community policing reduces crime. Braga, et. al, (2019) suggest that forms of policing disorder reduce crime via deterrence. Caton (2020) explores the social contract theory in the scope of moral obligations of our societal institutions and government agencies to protect the public and society's members. Donaldson, et. al (1994) suggest that businesses must identify, respect, and adhere to community mores, norms, and values to act as good corporate citizens as part of the social contract. Salter (2013) explores the Contractarian Anarchy theories of Buchanan juxtaposed with the social contract theory,

suggesting that individual members of society have the right to leave a societal community when that community fails to fulfill the social contract. The institutions of our society have a moral obligation to protect the members of society, and failure to do so harms the social order.

The ideal components of a model identity theft program could potentially reduce identity theft via an effective combination of prevention through education, victim assistance, and deterrence through enforcement. Current practices in the United States appear to focus on prevention and victim assistance with little or no follow-up investigation and enforcement, in effect removing any possibility of deterring potential perpetrators. This circumstance equates to institutional acceptance that victimization will occur, and signals to perpetrators that committing identity theft is low risk, as there is essentially no risk of discovery or accountability for the perpetrator. A multi-faceted approach that includes enforcement contends with each facet of identity theft, and should add discovery and accountability of perpetrators as potential forms of deterrence. While a model identity theft program including ideal components would not eliminate identity theft, it would certainly mitigate victimization from identity theft and could reduce the occurrence of identity theft incidents through its multi-faceted approach.

### **Limitations**

There were limitations encountered during the research for this paper. One evident limitation was a lack of specific data regarding identity theft incidents and follow-up of investigations, arrests, prosecutions, and case dispositions. Although improved data collection was included in the research recommendations for this paper, this research had to rely on less specific data from multiple data sources. Another limitation was that prevalent successful government identity theft programs appeared duplicative, and that these identity theft programs focused primarily on prevention and education, with victim assistance via education of victims

for recovery steps leaving victims to later help themselves. Although the predecessor program (OPP) to Wisconsin's current identity theft program of the Bureau of Consumer Protection was found to have enforcement and more direct involvement in victim advocacy efforts, this research could not obtain data/statistics for those efforts, and the OPP website and information could only be accessed via archive. This research was also limited in scope to identity theft programs used by and accessible to Wisconsin residents, and did not discover evaluations of current or past identity theft programs that would indicate the effectiveness of those specific programs.

### **Future Research**

For future research, it is recommended that additional data be obtained and analyzed specific to identity theft and identity theft-related crimes (e.g., credit card fraud, account takeovers, fraudulent establishment of accounts, etc.), including not just the number of incident reports filed, but also police reports made, investigations, arrests, prosecution referrals, prosecutions, and case dispositions, if and when such information becomes available. Future research could also expand in scope to identify and obtain information from program evaluations of identity theft programs not only from state and federal levels, but also from programs of foreign jurisdictions. Such information would identify the effectiveness of identity theft programs and the differences between markets and nations. Finally, future research into this area could also include data from potential new forms of identity theft; in particular, as cybertechnology advances in consumer products and services, the advancement also creates new opportunities for malfeasance (Dupont, 2016). All of this would help guide the formation of effective identity theft programs and inform ongoing improvements to achieve the desired outcomes of mitigating, preventing, and deterring identity theft.

## VII. Reference List

- 2020 elder fraud report - internet crime complaint center. (n.d.). Retrieved March 26, 2022, from [https://www.ic3.gov/Media/PDF/AnnualReport/2020\\_IC3ElderFraudReport.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf)
- Annual cases filings. Annual Cases Filings | Dane County Clerk of Courts. (n.d.). Retrieved March 26, 2022, from <https://courts.countyofdane.com/Court/Cases/2020>
- Annual report 2019 - Danesherriff.com. (n.d.). Retrieved March 24, 2022, from <https://www.danesherriff.com/documents/pdf/annual-report/2019-Annual-Report.pdf>
- Apau, Richard, & Koranteng, Felix Nti. (2019). Impact of Cybercrime and Trust on the Use of E-Commerce Technologies: An Application of the Theory of Planned Behavior. *International Journal of Cyber Criminology*, 13(2), 228–254. <https://doi.org/10.5281/zenodo.3697886>
- Baird, & Mayer, D. (2021). On integrative social contracts theory and corporate decision-making in a polarized political economy. *Business and Society Review* (1974), 126(1), 3–23. <https://doi.org/10.1111/basr.12223>
- Barnett-Ryan, Cynthia. (2002). The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data.
- Beaman, C., Barkworth, A., Akande, A.T., Hakak, S. & Khan, M.K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, 111, 1–. <https://doi.org/10.1016/j.cose.2021.102490>
- Bednar, Katos, V., & Hennell, C. (2009). The complexity of collaborative cyber crime investigations. *Digital Evidence and Electronic Signature Law Review*, 6, 214–. <https://doi.org/10.14296/deeslr.v6i0.1894>
- Betz-Hamilton. (2020). A Phenomenological Study on Parental Perpetrators of Child Identity Theft. *Financial Counseling and Planning*, 31(2), 219–228. <https://doi.org/10.1891/JFCP-19-00001>
- Bisogni, & Asghari, H. (2020). More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws. *Journal of Information Policy (University Park, Pa.)*, 10, 45–82. <https://doi.org/10.5325/jinfopoli.10.2020.0045>
- Bose, I., & Man Leung, A. C. (2019). Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly*, 43(1), 313–327. <https://doi.org/10.25300/misq/2019/14192>
- Braga, A. A., Welsh, B. C., & Schnell, C. (2019). Disorder policing to reduce crime: A systematic review. *Campbell Systematic Review*, 15(3). <https://doi.org/10.1002/cl2.1050>

- Brenner. (2006). Cybercrime jurisdiction. *Crime, Law, and Social Change*, 46(4), 189–206. <https://doi.org/10.1007/s10611-007-9063-7>
- Brown, C.S.D. (2015). Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 9(1), 55–.
- Buchanan, J. M. (1977). *Freedom in constitutional contract: Perspectives of a political economist*. Texas A & M University Press.
- Buchanan, & Musgrave, R. A. (1999). *Public finance and public choice two contrasting visions of the State / James M. Buchanan and Richard A. Musgrave*. MIT Press.
- Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports*, 17, 101058–101058. <https://doi.org/10.1016/j.pmedr.2020.101058>
- Caton. (2020). Moral Community and Moral Order: Developing Buchanan’s Multilevel Social Contract Theory. *Erasmus Journal for Philosophy and Economics*, 13(2), 1–29. <https://doi.org/10.23941/ejpe.v13i2.443>
- Cox. (2014). PROTECTING VICTIMS OF CYBERSTALKING, CYBERHARASSMENT, AND ONLINE IMPERSONATION THROUGH PROSECUTIONS AND EFFECTIVE LAWS. *Jurimetrics (Chicago, Ill.)*, 54(3), 277–302.
- BBB TIP: How to spot and avoid identity theft*. BBB. (n.d.). Retrieved April 5, 2022, from <https://www.bbb.org/article/news-releases/16951-bbb-tip-identity-theft>
- Bureau, U. S. C. (2022, March 24). *Data*. Census.gov. Retrieved March 26, 2022, from <https://www.census.gov/data.html>
- Chawki, Darwish, A., Khan, M. A., & Tyagi, S. (2015). Cybercrime: Introduction, Motivation and Methods. In *Cybercrime, Digital Forensics and Jurisdiction* (pp. 3–23). Springer International Publishing. [https://doi.org/10.1007/978-3-319-15150-2\\_1](https://doi.org/10.1007/978-3-319-15150-2_1)
- Cheng. (2021). The Distributed Hybrid Mathematical Model to analyze the theory of law and social control—A systematic case study approach. *Aggression and Violent Behavior*, 101634–. <https://doi.org/10.1016/j.avb.2021.101634>
- Chorghé, N., Jain, A., Mali, S., & Gunjgur, P. (2020). Identity Theft Prediction Using Game Theory. *ITM Web of Conferences*, 32, 3022. <https://doi.org/10.1051/itmconf/20203203022>
- Cingano Federico, & Tonello Marco. (2020). Law Enforcement, Social Control and Organized Crime: Evidence from Local Government Dismissals in Italy. *Italian Economic Journal*, 6(2), 221–254. <https://doi.org/10.1007/s40797-020-00124-1>

- City of Madison*. Self-Reporting System - City of Madison, Wisconsin. (n.d.). Retrieved March 22, 2022, from <https://www.cityofmadison.com/police/selfreport/selfreport.cfm>
- Cohn, Michael. (2017). IRS plans steps to curb ID theft. *Accounting Today*, 31(11), 40–40.
- Consumer Protection Fact Sheets*. DATCP Home Consumer Protection Fact Sheets. (n.d.). Retrieved April 5, 2022, from <https://datcp.wi.gov/Pages/Publications/ConsumerProtectionFactSheets.aspx>
- Cops office: Grants and Resources for Community Policing*. (n.d.). Retrieved March 26, 2022, from <https://cops.usdoj.gov/RIC/Publications/Publications/cops-p107-pub.pdf>
- Cross, Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, 518, 1–14.
- Cybercrime & Identity Theft Statistics 2021: Policy Advice*. Policy Advice. (2022, March 5). Retrieved March 27, 2022, from <https://policyadvice.net/insurance/insights/identity-theft-statistics/>
- Dane County District attorney*. Home Page | The Dane County District Attorney's Office. (n.d.). Retrieved April 5, 2022, from <https://da.countyofdane.com/>
- Dane County Sheriff's Office - Danesheriff.com*. (n.d.). Retrieved March 24, 2022, from <https://danesheriff.com/documents/pdf/annual-report/2008-Annual-Report.pdf>
- Data breaches*. DATCP Home Data Breaches. (n.d.). Retrieved April 3, 2022, from [https://datcp.wi.gov/Pages/Programs\\_Services/DataBreaches.aspx](https://datcp.wi.gov/Pages/Programs_Services/DataBreaches.aspx)
- The Definitive Guide to U.S. State Data Breach Laws*. (n.d.). Retrieved April 5, 2022, from <https://info.digitalguardian.com/rs/768-OQW-145/images/the-definitive-guide-to-us-state-data-breach-laws.pdf>
- DeLiema, Burnes, D., & Langton, L. (2021). The Financial and Psychological Impact of Identity Theft Among Older Adults. *Innovation in Aging*, 5(4), igab043–igab043. <https://doi.org/10.1093/geroni/igab043>
- District attorney*. District Attorney | Door County, WI. (n.d.). Retrieved April 5, 2022, from <https://www.co.door.wi.gov/184/District-Attorney>
- District attorney*. District Attorney | Kenosha County, WI - Official Website. (n.d.). Retrieved April 5, 2022, from <https://www.kenoshacounty.org/148/District-Attorney>
- Donaldson, & Dunfee, T. (1994). Toward a Unified Conception of Business Ethics: Integrative Social Contracts Theory. *The Academy of Management Review*, 19(2), 252–284. <https://doi.org/10.2307/258705>

Drew, & Farrell, L. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. *Police Practice & Research*, 19(6), 537–549. <https://doi.org/10.1080/15614263.2018.1507890>

Dupont. (2016). Bots, cops, and corporations: on the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law, and Social Change*, 67(1), 97–116. <https://doi.org/10.1007/s10611-016-9649-z>

Ellonen, Minkkinen, J., Kaakinen, M., Suonpää, K., Lee Miller, B., & Oksanen, A. (2020). Does Parental Control Moderate the Effect of Low Self-Control on Adolescent Offline and Online Delinquency? *Justice Quarterly*, 1–22. <https://doi.org/10.1080/07418825.2020.1738526>

*Fair credit reporting act - federal trade commission*. (n.d.). Retrieved April 3, 2022, from [https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a\\_fair-credit-reporting-act-0918.pdf](https://www.ftc.gov/system/files/documents/statutes/fair-credit-reporting-act/545a_fair-credit-reporting-act-0918.pdf)

FBI. (2016, June 17). *A brief description of the Federal Criminal Justice Process*. FBI. Retrieved April 4, 2022, from <https://www.fbi.gov/resources/victim-services/a-brief-description-of-the-federal-criminal-justice-process>

FBI. (2010, May 21). *Financial crimes 2008*. FBI. Retrieved February 19, 2022, from [https://www.fbi.gov/stats-services/publications/fcs\\_report2008](https://www.fbi.gov/stats-services/publications/fcs_report2008)

FBI. (2018, September 10). *Uniform crime reporting (UCR) program*. FBI. Retrieved February 12, 2022, from <https://www.fbi.gov/services/cjis/ucr>.

FBI. (2020, June 15). *Elder fraud*. FBI. Retrieved March 26, 2022, from <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud>

FBI. (2016, June 15). *Identity theft*. FBI. Retrieved April 3, 2022, from <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/identity-theft>

*Federal Trade Commission | protecting America's consumers*. (n.d.). Retrieved March 26, 2022, from [https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn\\_annual\\_data\\_book\\_2020.pdf](https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf)

*Financial crime (United States. Office of Justice Programs. Office for Victims of Crime)*. (2016). Office for Victims of Crime.

*Five things about deterrence*. National Institute of Justice. (n.d.). Retrieved March 27, 2022, from <https://nij.ojp.gov/topics/articles/five-things-about-deterrence>

Fligstein, & Roehrkasse, A. F. (2016). The Causes of Fraud in the Financial Crisis of 2007 to 2009: Evidence from the Mortgage-Backed Securities Industry. *American Sociological Review*, 81(4), 617–643. <https://doi.org/10.1177/0003122416645594>

- Free data visualization software. (n.d.). Retrieved February 12, 2022, from <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudandIDTheftMaps/IDTheftbyState>
- Golladay, K., & Holtfreter, K. (2016). The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders, 12*(5), 741–760. <https://doi.org/10.1080/15564886.2016.1177766>
- Georgiev. (2019). Profiling Human Roles in Cybercrime. *Information & Security, 43*(2), 145–160. <https://doi.org/10.11610/isij.4313>
- Graves, & Sexton, R. L. (2017). Optimal Public Policy Against Identity Theft. *The American Economist (New York, N.Y. 1960), 62*(2), 217–221. <https://doi.org/10.1177/0569434516682712>
- Green, Gies, S., Bobnis, A., Piquero, N. L., Piquero, A. R., & Velasquez, E. (2020). The Role of Victim Services for Individuals Who Have Experienced Serious Identity-Based Crime. *Victims & Offenders, 15*(6), 720–743. <https://doi.org/10.1080/15564886.2020.1743804>
- Guizzo, Danielle & Vigo de Lima, Iara. (2017). Polanyi and Foucault on the Issue of Market in Classical Political Economy: Complementary Approaches to the Radical Theory of Social Control. *The Review of Radical Political Economics, 49*(1), 100–. <https://doi.org/10.1177/0486613415621745>
- Gupta, C. M., & Kumar, D. (2020). Identity theft: a small step towards big financial crimes. *Journal of Financial Crime, 27*(3), 897–910. <https://doi.org/10.1108/JFC-01-2020-0014>
- Hill, & Marion, N. E. (2016). Presidential rhetoric on cybercrime: links to terrorism? *Criminal Justice Studies, 29*(2), 163–177. <https://doi.org/10.1080/1478601X.2016.1170279>
- Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer Fear of Online Identity Theft: Scale Development and Validation. *Journal of Interactive Marketing, 30*, 1–.
- Hirschi. (1969). *Causes of delinquency*. University of California Press.
- Holt, & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior, 35*(1), 20–40. <https://doi.org/10.1080/01639625.2013.822209>
- Identity theft*. Consumer Information. (2019, September 4). Retrieved February 12, 2022, from <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.
- Identity theft: Green bay, WI*. Identity Theft | Green Bay, WI. (n.d.). Retrieved April 5, 2022, from <https://greenbaywi.gov/1147/Identity-Theft>
- Identity theft: OVC*. Office for Victims of Crime. (n.d.). Retrieved April 4, 2022, from <https://ovc.ojp.gov/topics/identity-theft>

*Identity Theft Protection*. DATCP Home Identity Theft Protection. (n.d.). Retrieved February 12, 2022, from [https://datcp.wi.gov/Pages/Programs\\_Services/IdentityTheft.aspx](https://datcp.wi.gov/Pages/Programs_Services/IdentityTheft.aspx).

*Identitytheft.gov*. IdentityTheft.gov. (n.d.). Retrieved March 26, 2022, from <https://www.identitytheft.gov/#/>

*Internet crime complaint center(ic3) | Annual reports*. (n.d.). Retrieved February 12, 2022, from <https://www.ic3.gov/Home/AnnualReports>

*Internet crime complaint center(ic3) | Annual reports*. (n.d.). Retrieved March 26, 2022, from <https://www.ic3.gov/Home/AnnualReports>

Inusah, & Gawu, P. S. (2021). The Social Contract Theory and Corporation Moral Obligation. *E-Logos (Prague)*, 28(1), 4–16. <https://doi.org/10.18267/j.e-logos.480>

Jakubiec. (2020). Threats of identity theft in cyberspace - case study. *ASEJ Scientific Journal of Bielsko-Biala School of Finance and Law*, 24(2), 10–14. <https://doi.org/10.5604/01.3001.0014.3291>

Jian, Chen, S., Luo, X., Lee, T., & Yu, X. (2020). Organized Cyber-Racketeering: Exploring the Role of Internet Technology in Organized Cybercrime Syndicates Using a Grounded Theory Approach. *IEEE Transactions on Engineering Management*, 1–13. <https://doi.org/10.1109/TEM.2020.3002784>

Jordan, G., Leskovar, R., & Marič, M. (2018). Impact of fear of identity theft and perceived risk on online purchase intention. *Organizacija*, 51(2), 146–155. <https://doi.org/10.2478/orga-2018-0007>

Kerstens, & Jansen, J. (2016). The Victim-Perpetrator Overlap in Financial Cybercrime: Evidence and Reflection on the Overlap of Youth's On-Line Victimization and Perpetration. *Deviant Behavior*, 37(5), 585–600. <https://doi.org/10.1080/01639625.2015.1060796>

Kumar, & Shareef, M. A. (2012). Prevent/Control Identity Theft: Impact on Trust and Consumers' Purchase Intention in B2C EC. *Information Resources Management Journal*, 25(3), 30–60. <https://doi.org/10.4018/irmj.2012070102>

Lane, G. W., & Sui, D. Z. (2010). Geographies of identity theft in the U.S.: understanding spatial and demographic patterns, 2002-2006. *GeoJournal*, 75(1), 43–55. <https://doi.org/10.1007/s10708-010-9342-1>

*Learn more at measures for Justice*. Measures for Justice. (n.d.). Retrieved March 26, 2022, from <https://measuresforjustice.org/portal/WI025/measures/120?c=1>

Leighton-Daly, M. (2019). Identity theft and tax crime: has technology made it easier to defraud the revenue? *eJournal of Tax Research*, 16(3), 578–593.

- Leukfeldt, Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitised world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*, 22(3), 324–345. <https://doi.org/10.1007/s12117-019-09366-7>
- Maras, Marie-Helen. (2016). International cybercrime investigations and prosecutions: Cutting the gordian knot. *Pandora's Box*, 2016, 107–112.
- Milwaukee County district attorney. (n.d.). Retrieved April 5, 2022, from <https://county.milwaukee.gov/EN/District-Attorney>
- Milwaukee Police Department. Identity Theft. (n.d.). Retrieved April 5, 2022, from <https://city.milwaukee.gov/police/Police-Units-Partners/Financial-Crimes-Unit/IdentityTheft>
- Mironov. (2013). Taxes, Theft, and Firm Performance. *The Journal of Finance (New York)*, 68(4), 1441–1472. <https://doi.org/10.1111/jofi.12026>
- Moehler. (2018). Diversity, stability, and social contract theory. *Philosophical Studies*, 176(12), 3285–3301. <https://doi.org/10.1007/s11098-018-1174-8>
- Navarro, & Higgins, G. E. (2016). Familial Identity Theft. *American Journal of Criminal Justice*, 42(1), 218–230. <https://doi.org/10.1007/s12103-016-9357-3>
- Payne, & Kennett-Hensel, P. A. (2017). Combatting Identity Theft: A Proposed Ethical Policy Statement and Best Practices. *Business and Society Review (1974)*, 122(3), 393–420. <https://doi.org/10.1111/basr.12121>
- Pongsiri. (2002). Regulation and public-private partnerships. *The International Journal of Public Sector Management*, 15(6), 487–495. <https://doi.org/10.1108/09513550210439634>
- Pults. (2020). America's Data Crisis: How Public Voter Registration Data Has Exposed the American Public to Previously Unforeseen Dangers and How to Fix It. *Iowa Law Review*, 105(3), 1363–1409.
- Ren, Zhao, J. "Solomon", & He, N. "Phil." (2019). Broken Windows Theory and Citizen Engagement in Crime Prevention. *Justice Quarterly*, 36(1), 1–30. <https://doi.org/10.1080/07418825.2017.1374434>
- Romanosky, Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, 30(2), 256–286. <https://doi.org/10.1002/pam.20567>
- Salter, A. W. (2013). James Buchanan and Contractarian Anarchy. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2324373>

- Schultz, David. (2018). 401(K) PLANS: Where's My Money? An Upsurge in Identity Theft and Fraud Is Putting Participants, Plan Sponsors, and Recordkeepers at Risk. *Journal of Pension Benefits*, 26(1), 53–56.
- Seabright, Stieglitz, J., & Van der Straeten, K. (2021). Evaluating social contract theory in the light of evolutionary social science. *Evolutionary Human Sciences*, 3. <https://doi.org/10.1017/ehs.2021.4>
- Shah, Maitlo, A., Jones, P., & Yusuf, Y. (2019). An investigation into agile learning processes and knowledge sharing practices to prevent identity theft in the online retail organisations. *Journal of Knowledge Management*, 23(9), 1857–1884. <https://doi.org/10.1108/JKM-06-2018-0370>
- Shareef, M. A., Dwivedi, Y. K., Kumar, V., Davies, G., Rana, N., & Baabdullah, A. (2019). Purchase intention in an electronic commerce environment: A trade-off between controlling measures and operational performance. *Information Technology & People* (West Linn, Or.), 32(6), 1345–1375. <https://doi.org/10.1108/ITP-05-2018-0241>
- Staff, the P. N. O., & This blog is a collaboration between CTO and DPIP staff and the AI Strategy team. (2022, March 29). *Data breach response: A guide for business*. Federal Trade Commission. Retrieved April 3, 2022, from <https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business>
- Staff, the P. N. O., & This blog is a collaboration between CTO and DPIP staff and the AI Strategy team. (2020, March 4). *Fair credit reporting act*. Federal Trade Commission. Retrieved March 24, 2022, from <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act>
- Statement of rights for identity theft victims*. (n.d.). Retrieved March 24, 2022, from <https://ovc.ojp.gov/sites/g/files/xyckuh226/files/media/document/idtrightsbooklet.pdf>
- Steel, Chad M. S. (2019). Stolen Identity Valuation and Market Evolution on the Dark Web. *International Journal of Cyber Criminology*. Jan-Jun2019, Vol. 13 Issue 1, 70-83.
- Tcherni, Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, 33(5), 890–911. <https://doi.org/10.1080/07418825.2014.994658>
- Trost. (2017). The Impostor Rule and Identity Theft in America. *Law and History Review*, 35(2), 433–459. <https://doi.org/10.1017/S0738248017000074>
- Understanding restitution*. The United States Department of Justice. (2015, April 17). Retrieved April 4, 2022, from <https://www.justice.gov/usao-ndga/victim-witness-assistance/understanding-restitution>

U.S. Department of Health and Human Services. (n.d.). *Elder abuse*. National Institute on Aging. Retrieved March 26, 2022, from <https://www.nia.nih.gov/health/elder-abuse>

[USC02] 18 USC 1028: Fraud and related activity in connection with identification documents, authentication features, and information. (n.d.). Retrieved February 12, 2022, from <https://uscode.house.gov/view.xhtml?req=%28title%3A18+section%3A1028+edition%3Aprelim%29+OR+%28granuleid%3AUSC-prelim-title18-section1028%29&f=treesort&edition=prelim&num=0&jumpTo=true>

Van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. <https://doi.org/10.1177/1477370818773610>

White-Collar Crime. (2016, May 3). Retrieved March 24, 2022, from <https://www.fbi.gov/investigate/white-collar-crime>

Wisconsin Department of Justice. Criminal Litigation Unit | Wisconsin Department of Justice. (n.d.). Retrieved April 2, 2022, from <https://www.doj.state.wi.us/dls/criminal-litigation-unit>

Wisconsin Department of Justice. Domestic Abuse Data | Wisconsin Department of Justice. (n.d.). Retrieved April 1, 2022, from <https://www.doj.state.wi.us/dles/bjia/domestic-abuse-data>

Wisconsin Department of Justice. Public Protection Unit | Wisconsin Department of Justice. (n.d.). Retrieved April 2, 2022, from <https://www.doj.state.wi.us/dls/public-protection-unit>

Wisconsin Department of Justice. UCR Offense Data | Wisconsin Department of Justice. (n.d.). Retrieved February 12, 2022, from <https://www.doj.state.wi.us/dles/bjia/ucr-offense-data>.

Wisconsin Department of Justice. Wisconsin Department of Justice | WisDOJ. (2022, March 22). Retrieved March 22, 2022, from <https://www.doj.state.wi.us> > files > news-media

Wisconsin Department of Justice. UCR Arrest Data | Wisconsin Department of Justice. (n.d.). Retrieved March 26, 2022, from <https://www.doj.state.wi.us/dles/bjia/ucr-arrest-data>

Wisconsin Legislative Fiscal Bureau. (2019, January). *Consumer Protection Programs - Informational Paper*. January 2019. Retrieved April 5, 2022, from [https://docs.legis.wisconsin.gov/misc/lfb/informational\\_papers/january\\_2019/0084\\_consumer\\_protection\\_programs\\_informational\\_paper\\_84.pdf](https://docs.legis.wisconsin.gov/misc/lfb/informational_papers/january_2019/0084_consumer_protection_programs_informational_paper_84.pdf)

Wisconsin legislature: Chapter 100. (n.d.). Retrieved April 7, 2022, from <https://docs.legis.wisconsin.gov/statutes/statutes/100>

Wisconsin legislature: 943.201. (n.d.). Retrieved February 12, 2022, from <https://docs.legis.wisconsin.gov/statutes/statutes/943/iii/201>

Wisconsin Office of Privacy Protection. (n.d.). Retrieved April 5, 2022, from <https://web.archive.org/web/20080328040936/http://privacy.wi.gov/complaints/complaints.jsp>

Wisconsin Office of Privacy Protection. (n.d.). Retrieved April 1, 2022, from [https://web.archive.org/web/\\*/www.privacy.wi.gov](https://web.archive.org/web/*/www.privacy.wi.gov)

Yenouskas, & Swank, L. W. (2018). Emerging Legal Issues in Data Breach Class Actions. *The Business Lawyer*, 73(2), 475–485.

Zaiss, J., Nokhbeh Zaeem, R., & Barber, K. S. (2019). Identity Threat Assessment and Prediction. *The Journal of Consumer Affairs*, 53(1), 58–70.  
<https://doi.org/10.1111/joca.12191>

