laws

MDPI

Article

Identity Theft: The Importance of Prosecuting on Behalf of Victims

Christopher S. Kayser [1,*], Sinchul Back [2] and Marlon Mike Toro-Alvarez [3]

[1] Cybercrime Analytics Inc., Calgary, AB T2S 2Z3, Canada
[2] Department of Criminal Justice, Cybersecurity & Sociology, The University of Scranton, Scranton, PA 18510, USA; sinchul.back@scranton.edu
[3] School of Justice and Public Safety, Southern Illinois University, Carbondale, IL 62901, USA
* Correspondence: ckayser@cybercrimeanalytics.com

Abstract: Rates of victimization from identity theft continue to rise exponentially. Personally identifiable information (PII) has become vitally valuable data bad actors use to commit fraud against individuals. Focusing primarily on the United States and Canada, the objective of this paper is to raise awareness for those involved in criminal justice (CJ) to more fully understand potential life-changing consequences for those whose PII is used fraudulently. We examine the impact of crimes involving PII and the urgent need to increase investigations and legal proceedings for identity theft-related crimes. Referring to a National Crime Victimization Survey, we analyze why many victims of identity theft crimes resist notifying appropriate authorities. We also address why those within the CJ system are often reluctant to initiate actions against occurrences of identity theft. We provide insight into consequences experienced by identity theft victims, particularly if their PII is posted on the Dark Web, a threat that can exist into perpetuity. If rates of victimization from identity theft-based crimes are to decline, reporting of victimization must increase, and current legislation related to investigating and processing identity theft crimes must progress.

Keywords: criminal justice system; CJ; identity theft; personally identifiable information; PII; victimization

Citation: Kayser, Christopher S., Sinchul Back, and Marlon Mike Toro-Alvarez. 2024. Identity Theft: The Importance of Prosecuting on Behalf of Victims. *Laws* 13: 68. https://doi.org/10.3390/laws13060068

Academic Editor: Patricia Easteal

Received: 4 July 2024
Revised: 18 October 2024
Accepted: 31 October 2024
Published: 7 November 2024

1. Introduction

For the purposes of the current study, the authors define identity theft as using someone's PII to commit fraud. Furthermore, we define PII as any information that can be specifically associated with a specific individual. Additional definitions of identity theft and PII are described in Section 2.1.

Crimes involving identity theft are not a new phenomenon, and rates of victimization continue to escalate. Studies have suggested that one in three Americans will experience some form of identity theft during their lifetime (Identitytheft.org 2024). Increased adoption and dependence on technology, as well as greater requirements to disclose PII, are fueling increasing occurrences of identity theft (Insurance Information Institute 2024; McCants and Golanka 2024; Statista 2024). Currently, there exist gaps in research and industry to sufficiently address identity theft victimization (Muniz et al. 2024).

From 2013 to 2023, Internet users have grown from two-and-one-half billion to over five billion, and smartphone users have increased from nearly three billion to six billion (Seitz 2024; Statista 2023). As of 2023, social media users exceeded five billion worldwide (Statista 2023). As revealed in studies by the U.S. Bureau of Justice (BJS) and the U.S. Department of Justice (DOJ), massive growth rates provide increasingly greater sources of PII that threat actors and cybercriminals can target and use for illicit purposes, resulting in spiraling global rates of identity theft victimization (BJS 2023; DOJ 2023).

Individuals of all ages can be harmed by the illicit use of their PII. Victimization can occur in many forms: financial, non-financial, and criminal record (White and Fisher 2008).

The majority are conducted using email, on social media sites, or the Internet through sexual scams, bullying, and other predatory crimes (Whitty and Buchanan 2012). An estimated 24 million people in the United States were victims of some form of identity theft in 2020, with 15 percent suffering $16.4 million in losses (Harrell and Thompson 2023a). The (BJS) reported that in 2023, 59 million Americans over the age of 16 had been victims of identity theft at least once in their lifetime (ibid.).

Reported data compromises in the U.S. dropped from 1862 in 2021 to 1802 in 2022. An estimated 422 million individuals were affected by these events. Although the drop in the number of compromises appears encouraging, since 2019, the reporting of identity theft breaches has declined by 50 percent. Data from a BJS survey suggests that more identity theft crime is occurring than is being reported (BJS 2023), resulting in statistics being skewed in relation to actual victimization rates (ITRC 2023b).

The current study examines the impact of being victimized by identity theft crimes, particularly as it pertains to PII. We provide a review of existing literature related to identity theft and how those in CJ have historically dealt with identity theft crimes. Next, we address ways that PII can be acquired or stolen and examine how improved capable guardianship can better protect this important data. A brief discussion of the market value of PII on the Dark Web follows (Balaji 2018; IBM 2023; Liu et al. 2023; Zolton 2023). Differences between the surface web, deep web, and Dark Web reveal varying risks associated with each platform in relation to Internet usage and how stolen PII can be made available into perpetuity on the Dark Web (Liu et al. 2021; Veltman 2024). The effects of victimization from fraudulent use of PII are addressed, followed by our analysis of data from a National Crime Victimization Study conducted by the BJS (2023) to analyze why reporting rates of victims of identity theft remain low. A review of major data breaches reveals the immensity of PII that can be acquired through data breaches and subsequent financial penalties against organizations who failed to sufficiently protect entrusted PII (Hill and Swinhoe 2022; Krebson Security 2023; Madnick 2024; C. Page 2021). Finally, we focus on the challenges faced by CJ organizations and individuals related to initiating legal actions for identity theft-based crimes (Carson and Cameron 2023; Macnab 2022; Gelowitz et al. 2021). Based on the current study, we summarize our research and findings and offer suggestions on how those involved in CJ could become more effective in addressing identity theft crimes. We conclude by emphasizing that further research is recommended to encourage changes to existing CJ legislation to provide more effective measures to investigate and commence legal actions against those engaged in identity theft and fraudulent use of PII (Arnell and Faturoti 2023; Kello 2021). Such improvements are of particular importance as they relate to large data breaches and potential class-actions.

2. Literature Review

Extant research focusing on identity theft, and the need for those in CJ systems to become more proactive in investigating and prosecuting those responsible for illegally obtaining PII, committing crimes using PII, or failing to protect PII that has been entrusted to them, requires significant changes to existing practices and legislation (Kello 2021; Koops 2012). Many studies have focused on identity theft crimes using PII, increasing rates of victimization, and physical and psychological harms experienced by victims of identity theft (Irvin-Erickson 2024). The importance of protecting PII, how it is used to commit fraud, and how identity theft crimes are being addressed by the CJ system has been widely researched (Allison 2003; Copes et al. 2010; Guedes et al. 2023; Hoar 2001; Koops and Leenes 2006; Li et al. 2019; Perl 2004). However, due to a wide array of methods for examining identity theft crimes, continued research is required if we are to better understand the consequences for victims of identity theft, and how all areas of CJ can become more effective at addressing crimes involving PII (Irvin-Erickson 2024).

Increasingly, private, public, and government organizations require individuals to submit PII for account information and verification, personal and credit checks, and numerous other verification purposes. In Canada, the use of customer's personal information used

to provide services increased from 63 percent in 2019 to 84 percent in 2023 (OPC 2024b). A 2019 PEW Research Center study revealed most Americans are concerned about their PII being collected by companies and the government. Their major concerns relating to companies and the government were: (1) not having control over the collection of their personal data by companies (81 percent) and the government (84 percent); (2) believing risks outweigh the benefits of collecting their PII (81 percent companies, 66 percent the government); (3) concerned about how their PII is collected (79 percent companies, 64 percent the government); and (4) how their PII would be used (59 percent companies, 78 percent the government) (PEW Research Center 2019).

Such requirements have resulted in an increase in PII being stored by organizations that are often not sufficiently secured. Simultaneously, bad actors have become more effective in circumventing security efforts to protect PII. Further research related to the impact of identity theft crimes is urgently required to increase awareness of the need to more effectively protect entrusted PII, and for those in CJ to be more responsive to investigate and prosecute occurrences of crimes involving identity theft.

Several studies have addressed identity theft as it pertains to the need to protect PII, victimization consequences, how a law enforcement agency (LEA) has responded and the need for improved methods of response, and how identity theft-based crimes are handled by the courts (Burnes et al. 2020; Finklea 2014; Hoar 2001; Newman and McNally 2005). Identity theft is a major crime that can cause irreparable harm to those whose PII is used fraudulently (Burnes et al. 2020; DiNardi 2023; Golladay and Holtfreter 2017; Harrell and Thompson 2023b; Li et al. 2019; Randa and Reyns 2020; Rubenking 2022). There is an immediate need for improvements within CJ systems in responding to and initiating criminal proceedings against those who commit these crimes if victimization rates are to decline (Kello 2021).

This paper aims to expand upon existing research on four important topics. First, how PII is becoming an increasingly important element to commit fraud. Second, that the availability of PII on the Dark Web is expanding, as is the value of such information when used for illicit purposes. Third, why victims of identity theft, once aware their PII has been stolen, or when victimized through an identity theft crime, are largely reluctant to contact authorities to file a report (BJS 2023). Fourth, examining ongoing challenges faced by those within the CJ system that contribute to a reluctance to investigate and prosecute incidents involving compromised or stolen PII (Shinder 2011).

2.1. Identity Theft and PII

Identity theft is becoming more prevalent with increasing advancements in technology and how we rely on technology when communicating. Consequently, our willingness to increasingly share our PII, voluntarily or when requested to do so, continues to exponentially fuel occurrences of PII theft. There are many definitions of identity theft and PII, including, but not limited to:

A 2004 Federal Trade Commission (FTC) report defined identity theft as "a fraud that is committed or attempted, using a person's identifying information without authority" (FTC 2004). In 2021, the FTC further defined identity theft as "...the intentional, unauthorized use of a person's identifying information for unlawful purposes" (DeLiema et al. 2021).

A recent National Crime Victimization Survey (NCVS) conducted by the BJS identified three examples of identity theft as the: unauthorized use or attempted use of an existing account; unauthorized use or attempted use of personal information to open a new account; and misuse of personal information for a fraudulent purpose (BJS 2022).

The FTC 2023 Consumer Sentinel Network Data Book identified the top three types of identity theft that occurred from 2018 to 2022 for 2,849,962 reported cases as: credit card fraud (1,654,850); loan or lease fraud (713,333); and bank fraud (481,779) (FTC 2023a). Of 1,108,609 reported cases in 2022, 81 percent were reported by those 20 to 59 years of age (ibid.). Financial losses reported by identity theft victims during this period totaled nearly

nine billion dollars (ibid.). From 2019 to 2022, personal data breaches reported to the FBI rose 65 percent, from 38,218 to 58,859 (FBI 2022).

The National Institute of Standards and Technology (NIST) of the U.S Department of Commerce defines personally identifiable information (PII) as:

> Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's given name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (NIST 2020)

The *California Penal Code* Part 1, Title 13, Chapter 8, Section 530.5 defines identity theft as:

> Every person who willfully obtains personal identifying information, as defined in subdivision (b) of Section 530.55, of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services, real property, or medical information without the consent of that person. (California Legislative Information 2023)

2.2. How PII Is Acquired

As described in Cohen and Felson's Routine Activity Theory (RAT), a crime is likely to occur when three factors converge in time and space: a motivated offender, a suitable target, and the absence of capable guardianship (any person or thing that discourages criminal violations from occurring) (Cohen and Felson 1979). In the event a crime is committed using technology or the Internet, crime can progress from physical contact to electronic communications, increasing the target pool of possible victims exponentially (Leukfeldt and Yar 2016).

Choi's (2011) cyber-routine activities theory (Cyber-RAT) expands upon Cohen and Felson's RAT, addressing the technological aspects of computer crime and cyber-victimization by examining people's online conduct and aspects of their digital guardianship as it relates to cyber-victimization—a significant contributor to rising rates of cyber-victimization.

Kayser's (2020) RESCAT (Required Elements for a Social Engineered Cyber-Attack Theory) also expands upon Cohen and Felson's RAT, investigating how cybercriminals utilize elements of human nature and human curiosity to socially engineer users of technology (UoT) to grant illicit access to a target's information, particularly PII, that can be used for illicit purposes (Kayser et al. 2020). Kayser's (2020) continuing research into how elements of social engineering are incorporated into most cyber-attacks by cybercriminals, addresses the rise in cyber-victimization through illicit use of PII.

As with any crime, the more conditions which exist that increase the vulnerability of someone targeted for criminal purposes, the greater the probability they will be victimized. A lack of understanding by individuals of the importance of adequately protecting their PII, particularly when interacting electronically with others on social media, texting, emailing, shopping online, or accessing unknown websites on the Internet, compounds the risk of having their PII acquired for illicit purposes (Choi 2011; Harrell and Thompson 2023b; Kayser 2020; Kayser et al. 2020).

Other research suggests there are three forms of capable guardianship that individuals can engage in to help reduce the risks of their PII being acquired:

(1) passive physical guardianship (using anti-virus software and browsing securely);
(2) active personal guardianship (proper management of passwords); and
(3) avoidance of personal guardianship by reducing online activities such as online banking and shopping, and generally spending less time on the Internet (Williams 2015).

PII acquired by bad actors is regularly publicized on the Dark Web, where it can remain available for sharing or sale, typically for criminal purposes, unless the site that hosts the information goes dark (closes) (Liu et al. 2021).

PII can be obtained physically and electronically. Physical thefts often target computers, storage devices, cell phones, documents, backpacks, purses, and wallets. Observing someone displaying visible hard copies of their PII or online activities is referred to as shoulder surfing.

Examples of electronic acquisitions of PII include: accidental sharing of data (faxing and other transmission errors), ransomware, and other forms of cyberattacks that attempt to infiltrate corporate information or customer databases (data at rest).

Increasingly, cyberattacks are the most common means of illicitly acquiring PII, representing over 90 percent of all data breaches in 2022 (ITRC 2023b). Masterfully executed social engineering techniques can beguile individuals to voluntarily provide or forfeit access to their PII via email, text, and cellphone communications utilizing social engineering techniques such as phishing, spear phishing, Smishing (text message phishing), Vishing (voice and voicemail phishing), baiting, Business Email Compromise (BEC), honeytraps, romance scams, scareware, watering hole attacks, and whaling (Jones 2023a; Kayser 2020; Kayser et al. 2020).

The two most common methods for cybercriminals to exfiltrate PII from large networks or databases are through hardware and software (malware) attacks and social engineering individuals associated with targeted organizations. Failure to keep hardware and software updated, especially as it pertains to new versions addressing known vulnerabilities, can provide open access to circumvent anti-intrusion programs. Malicious software such as ransomware, keyloggers, worms, and various forms of viruses can also facilitate unfettered access to data if firewalls are successfully infiltrated.

Even the most efficiently protected networks and databases can be accessed by astute cybercriminals taking advantage of zero-day events (occasions where access can be gained for only a brief period of time before a security flaw is corrected—often as a result of hardware or software update errors by a manufacturer).

An independent IT security institute reported that over one billion versions of malware and 200 million potentially unwanted applications (PUA) were detected in 2023—an alarming increase of 95 percent and 99 percent, respectively, since 2011 (AVtest 2023). Another report noted that over 500,000 new malwares are detected every day (Chen 2023; Jovanovic 2023).

Next, we address the value of PII and why it is coveted by those who wish to commit identity theft crimes.

2.3. Determining the Value of PII

Social media companies such as Google and Meta rely heavily on PII, specifically user data, to generate billions of dollars in advertising revenue annually. An email address can be sold to marketing companies for as much as $89 (Liu et al. 2023). When used for illicit purposes, PII is equally valuable to criminals. The creation of fictitious accounts can be carried out by stealing someone's existing account and creating a false representation or by hacking a legitimate account by taking over the owner's access to their personal account (Lach 2014).

PII has been classified as direct identifiers and non-direct identifiers, and sensitive and non-sensitive. Direct identifiers are unique to an individual, such as a driver's license or passport number, with only one often being sufficient to identify someone. Non-direct identifiers such as race, birthplace, zip code, and gender are not unique and do not pose the same threat of possible victimization on their own, as each identifier will not positively identify someone specifically. However, when combined with other non-direct PII, someone's identity can be confirmed (IBM 2023).

Sensitive PII can prove harmful to the individual. Examples include: SSN; driver's license and passport numbers and other government-issued identification; biometric identification; medical records and financial information—information that is usually not made public (ibid.).

Attempts to commit a crime using one piece of non-sensitive PII would not normally be considered useful on its own, but if combined with additional non-sensitive PII, it can become much more valuable in efforts to commit fraud. Examples include: a person's full name, mother's maiden name, phone number(s), place and date of birth, personal and email addresses, race, ethnicity, or religion. A creative criminal could successfully access someone's bank accounts using the following process:

> [A] hacker could break into someone's bank account app with their phone number, email address, and mother's maiden name. The email gives them a username, spoofing the phone number gives them a way to receive a verification code, and the mother's maiden name gives them an answer to the security question. (ibid.)

The value of PII can vary greatly. Prices for PII are determined by who possesses the data and those interested in acquiring it. As previously noted, certain PII can demand higher prices if those in possession can attest to the validity of the data by testing it in real-life situations. This raises the confidence level of purchasers that there is a high probability that illicit use of the data should pass security checks. Examples include credit and debit cards, usernames and passwords, passports, medical information, employment status, and histories, among other types of PII.

Cybersecurity firms Privacy Affairs scans the Dark Web for information related to prices charged for stolen PII and other data. Their extensive 2023 report listed asking prices for hundreds of types of PII and other data. Examples include: 7.5 million credit cards varying from $70 to $110 (depending on credit limits), payment processing services—$10 to $4255, crypto accounts—$20 to $2650, social media accounts—$1 to $60, forged drivers licenses—$20 to $140, forged passports—$3000 to $4000, email database dumps—$100 to $200, and hacked cryptocurrency accounts—$70 to $1170 (Zolton 2023).

Data stolen in 2018 in a Chinese hotel breach garnered cybercriminals over 200 million highly sensitive PII data, which were subsequently advertised for sale on the Dark Web for approximately US$58,000 (Balaji 2018). Three sets of data were available for purchase: 123 million records containing names, mobile phone numbers, email addresses, identity theft numbers, and residential addresses; 130 million records containing registered check-in-time, customer name, identity theft number, home address, birthday, and internal identity theft number; and 240 million records containing customer names, room numbers, card numbers, mobile numbers, email addresses, check-in and departure times, and hotel identity theft numbers (ibid.).

Another report associated with the Chinese hotel breach highlighted additional information that was available from this breach: student-, hotel-, and financial investment-related PII that included full names, Alipay accounts, WeChat bills, debit card, and other financial information; banking and identity theft information, shown with people holding the cards (as a form of identification); PII of beauty pageant contestants, including names, attributes, and social media accounts; stolen Taiwanese and Brazilian credit card data for which payment could be sent to the person's Steam account; Chinese national passports; and personal pictures of young women using QQ accounts (Trend Micro 2018).

More recently, two significant cyber breaches resulted in illegally acquired data being posted quickly on the Dark Web. On 28 April 2014, London Drugs, a Western Canadian major pharmacy, electronics, grocery, health and beauty products, and housewares chain with 79 stores and over 8000 employees, experienced a ransomware attack by the ransomware gang known as LockBit. As a means to pressure London Drugs to pay the requested $25 million dollar ransom, LockBit posted the breach on their data leak site, giving London Drugs 48 h to pay, or LockBit would post a 300 gigabyte folder on the Dark Web containing information related to London Drugs employees that included "files on payrolls, garnishments, pay stubs, taxes, benefits, sick leaves, suppliers' names, photos, invoices, meeting minutes, billings, executive calendars, letters, emails, and presentations", as well as investigations of harassment from their human resources department, including named parties (Harnett 2024). As a result of the cyberattack, London Drugs closed its entire chain of stores for 10 days for security reasons and related recovery efforts.

Of even greater consequence was a cyber breach that occurred on 20 May 2024, in which the cybercrime group known as ShinyHunters infiltrated a third-party cloud storage database and gained access to Live Nation's Ticketmaster accounts for nearly 560,000 customers. Demands for a ransom payment of US$500,000 to prevent the hackers from advertising the stolen data on the Dark Web for sale were ignored, resulting in the data being posted on the Dark Web for a one-time sale, just days after the attack. Ticketmaster's customer information offered for sale included names, addresses, phone numbers, and partial credit card information (Sky News 2024).

2.4. Defining Surface Web (Internet) and Dark Web

Due to extensive referencing of the Internet and Dark Web throughout this paper, we offer definitions and a brief history for readers. Important takeaways from this history are the immense growth of the Dark Web, and the inability for LEAs to effectively impact the ongoing criminal aspects and activities related to its existence.

The majority of those who access the Internet using the surface web (World Wide Web, "www") use standard web browsers such as Firefox, Google Chrome, Microsoft Edge, Internet Explorer, Safari, or Opera, which do not require specific authorizations or software to use. Such access represents about 10 percent of all users of the Internet. When accessing the surface web, one's identity is commonly visible (although people can create pseudonyms to maintain anonymity). It is important for those accessing the surface web to be aware that publicized PII can be easily acquired by bad actors who will then use the Dark Web to publish and share such information anonymously. The Dark Web is a heavily encrypted platform that is part of the Deep Web, which represents about 90 percent of the entire World Wide Web (Basheer and Alkhatib 2021).

Much research has been conducted regarding the history, present status, and future outlook of the Dark Web (Beshiri and Susuri 2019; Guccione 2024; Oliver 2024; Raman et al. 2023). The modern form of the Dark Web has been in existence since 2009, but its origin dates back to the 1960s with the creation of ARPANET—a method to share information over long distances without using phone connections (Kastner 2020). Today, the Dark Web is accessed through The Onion Router (TOR). It is used by LEAs, governments, and millions of others for legitimate purposes. However, recent studies have shown that up to 60 percent of those using the Dark Web do so obscurely and with anonymity to prevent detection, most often for illicit purposes (Acton 2024; Guccione 2024; Volle 2024).

Since its inception, cybercriminals have utilized the Dark Web to gain access to stolen PII and typically use digital currencies to facilitate transactions. As noted previously, many sellers on the Dark Web will first test data for sale to ensure its validity, thereby increasing their reputation of offering legitimate data, which allows them to increase asking prices for the data (Reflectiz 2024).

Stolen PII can be distributed via numerous apps, such as WhatsApp, Telegram, Google, Facebook, and others. However, the more common method is distribution on the Dark Web, primarily due to the longevity of its availability on the Dark Web. Once publicized, such information can be re-sold into perpetuity (Muniz et al. 2024). AT&T revealed in mid-March 2024 that PII for more than 70 million of its customers was illegally obtained in a 2019 (or earlier) data breach. Accessed data included: social security numbers, full names, email and mailing addresses, phone numbers, dates of birth, as well as AT&T account numbers and passcodes that was recently posted on the Dark Web—some that had been obtained up to five years earlier. Two previously acknowledged breaches of AT&T customer PII occurred in August 2021 (70 million customers' PII—not related to the 2019 breach, and which AT&T reportedly disputed happening) and March 2023 (9 million customer's PII) (Veltman 2024).

Despite multiple efforts by LEAs to shut down the Dark Web, it continues to flourish. The Silk Road, created and operated by Ross William Ulbright from 2011 to 2013, became the first major Dark Web market to offer illicit goods and services for sale, generating hundreds of millions of dollars in sales and $13 million in Bitcoin commissions. When

finally closed by the FBI, over one billion dollars in digital currencies were seized (FBI n.d., 2017). Following the Silk Road's demise, AlphaBay, operating from 2014 to when it was shuttered by the FBI in 2017, was the next kingpin of illicit marketplaces on the Dark Web. It was used to purchase weapons, drugs, hacking software, PII, and other illicitly obtained information, growing to ten times the size of the Silk Road (Ng 2017). The challenges for LEA to locate and terminate the Dark Web's illegal goods marketplaces shifted next to the Hansa Market, where many cybercriminals transitioned after AlphaBay was shuttered, with transactions on the Hansa Market increasing immediately by eight-fold; an increase anticipated by LEAs, resulting in the Hansa Market being terminated, within days of the demise of AlphaBay (ibid.).

Efforts by LEAs to shut down websites on the Dark Web offering illicit data remain increasingly more challenging, as new websites replace those that are voluntarily closed, or terminated by LEAs (Zolton 2023). Because many servers are used to conduct operations on the Dark Web, if all servers are not successfully located and closed, the operation can continue to function as other servers fill in to compensate for those eliminated (R. Page 2023). Dark Market, a major Dark Web criminal group operated by Genesis Market offering stolen credentials, was found to have nearly 500,000 users and 2400 sellers who had transacted over 320,000 times selling valuable information that could be used for criminal activities (ibid.). While there is no way to determine precisely how many websites exist on the Dark Web that offer illegally obtained or banned products, services, and data, recent estimates suggest of the approximately 30,000 hidden websites on the Dark Web, five percent are involved in illegal activities (Beckman 2023), making efforts to shut down this conduit of illicit products virtually an exercise in futility (Reflectiz 2024).

2.5. Effects of PII Victimization

Most commonly, those whose PII has been acquired for illicit purposes are not made aware until a fraud has occurred using their PII (Harrell and Thompson 2023b; Muniz et al. 2024). The theft and illicit use of someone's PII can cause significant harm to victims: financial, emotional and physical, medical information and access to health services, reputational, and life-altering adjustments required to address the impacts of victimization (Muniz et al. 2024). Examples of regularly targeted PII include: academic records, bank accounts, credit cards, credit lines, credit ratings, driver's licenses, government-issued identification, medical identification and information, mortgages, online shopping sites, personal loans, passports, professional and personal memberships, social media accounts, and other information related to someone's identity. A 2023 FTC report revealed the creation of fake government documents and claims represented the largest increase in identity theft claims, increasing 68 percent since 2022 (Akin 2024). Once compromised, victims will face a lifelong obligation to monitor everything related to their PII to reduce the risk of being harmed financially or reputationally (DiNardi 2023; Randa and Reyns 2020; Rubenking 2022).

2.6. Resulting Harm from Identity Theft

2.6.1. Emotional and Physical

The mental anxiety associated with dealing with PII-related crimes and the time and costs to dispute illegal transactions involving a victim's name have been shown to cause serious emotional harm and introduce new physical ailments as their health is challenged due to extreme levels of stress (Burnes et al. 2020; Golladay and Holtfreter 2017; Harrell and Thompson 2023b; Muniz et al. 2024). These symptoms are often more pronounced for victims of identity theft over age 65 (DeLiema et al. 2021). An additional challenge for individuals is the responsibility to become aware that their PII has been acquired for illicit purposes which is primarily their own responsibility (Muniz et al. 2024). Given the longevity of stolen PII that can exist in perpetuity on the Dark Web, this responsibility can be nearly impossible to achieve, until the discovery that they have become a victim.

Perceived and anticipated stress of worrying about how one's PII may be used maliciously into the future can cause victims' psychological state to be negatively impacted, resulting in lifelong anxiety (Li et al. 2019). Additional research has shown that being victimized by an identity theft crime has caused people to develop new medical issues or physical ailments (Randa and Reyns 2020), and serious physical and mental health morbidities have been associated with identity theft victimization (Burnes et al. 2020; DeLiema et al. 2021). For older victims, such processes can prove even more difficult, as their lifelong history with organizations with whom their PII was compromised could complicate attempts to contest unauthorized transactions.

One in 10 identity theft victims (approximately 2.6 million people) reported experiencing severe emotional distress following victimization (Harrell 2019). A quarter of identity theft victims experienced sleep problems, anxiety, and irritation six months after the crime (Sharp et al. 2004), with older adults and minorities experiencing more severe emotional consequences, including depression, anger, worry, and a sense of vulnerability (Golladay and Holtfreter 2017).

Research conducted by the Identity Theft Research Center (ITRC) found that negative feelings or emotions increased from 79 percent in 2021 to 87 percent for those who became aware their PII had been stolen. Emotions experienced by victims who responded to an ITRC 2022 survey included (in order of magnitude): worried or anxious (80%); violated (74%); angry (72%); vulnerable (70%); loss of trust (55%); sad or depressed (49%); shame or embarrassment (40%); guilt (33%); and suicidal (10%) (ITRC 2023a).

2.6.2. Financial, Non-Financial, and Criminal Record Identity Theft Fraud

Forms of financial identity theft fraud include: using PII to steal funds from or opening false accounts with financial institutions, credit card fraud, lines of credit or mortgage fraud (ABS 2024; Muniz et al. 2024; White and Fisher 2008). In cases where a mortgage is fraudulently taken out in someone else's name, it becomes the victim's responsibility to prove that they did not request the mortgage. This risk has become greater with the advent of digital mortgages, where little to no personal contact occurs between the borrower and the lender (Martin 2019).

If someone's tax identification number, such as their SSN, is used unlawfully, new identities, known as synthetic identity theft, can be created using that information, resulting in social security benefit claims being submitted or redirected to scammers (Jones 2023b; Ravichandran 2023).

Non-financial identity theft fraud involves someone using another person's PII to gain access to someone's medical information or health benefits or commit fraud by accessing services used by another person, such as telecommunications, utilities, or other services (White and Fisher 2008).

Criminal record fraud occurs when someone commits a crime or illegal activity, and when required to provide identification, they provide information pertaining to someone else's PII (ibid.).

2.6.3. Life-Altering Adjustments

Anyone whose PII has been acquired for criminal purposes will become subjected to potentially life-altering outcomes. Personal or corporate email accounts can be manipulated or taken over and used by others, health benefits can cease, loans and new credit cards can be opened, and personal mail can be redirected, often by simply requesting an address change to be made to the victim's accounts, thereby circumventing notification to the victim that this has occurred (Mandelblit 2001).

After a breach of their PII, limiting their activities to protect their PII ceases to be an option, requiring regular monitoring to guard against future victimization (Harrell and Thompson 2023b).One study revealed that over a 12-month period, 90 percent of those over 16 surveyed had taken at least one preventative action in an effort to keep their PII from being compromised (ibid).

2.6.4. Medical Information and Access to Health Services

Illegally acquired medical PII can be used by others for doctor visits, receiving medical procedures or other services, medications, and filing false medical reimbursement claims. Contamination of a victim's medical history can result in false medical information being included in the victim's records that could result in incorrect treatment by emergency responders, medical practitioners, or surgeons (Stein 2023). Using someone else's medical information to file false claims to insurance companies contributes to higher health insurance costs, and could result in someone being refused reimbursement for future legitimate claims under their health coverage or their coverage being canceled altogether (FTC 2011).

2.6.5. Reputational

When someone's PII is used to commit fraud, the costs and processes they must endure to prove they did not do the transaction, and to re-establish their personal credibility with organizations, can be a lengthy and extensive procedure (Schmitz 2008; Harrell and Thompson 2023b). In extreme cases, non-servicing of debt attributed to victims of identity theft can lead to a criminal record if victims, unaware that fraudulent financial transactions have occurred using their PII, are not aware of new payment obligations related to fraudulent transactions until notified by the lender or collection agencies. In the event that funds stolen from a financial institution, or a credit card are used illegally, victims can be involved in complex processes to prove they did not execute the transaction (Harrell and Thompson 2023b).

Finally, adding to all of these challenges for victims of identity theft, the burden of uncertainty of not knowing if their PII is being used within their own country or elsewhere can be impossible to verify, unless made aware that they have been victimized through illicit use of their PII. Notification of such fraudulent activities can take time or may never occur.

2.7. Research on Identity Theft

Previous research revealed that article searches of the Lexis-Nexis "US newspapers" database using the phrase "identity theft" rose from 95 articles in 1995, to almost 2000 in 2000, and over 12,000 in 2005 (Anderson et al. 2008). A 2001 Assistant United States Attorney bulletin stated many consider identity theft "the crime of the new millennium" [that can be] "accomplished anonymously, easily, with a variety of means, and the impact upon the victim can be devastating" (Hoar 2001).

Literature on identity theft, both conceptual and empirical, has been conducted for two decades. Most research on identity theft focuses on demographic characteristics, including age, gender, race, income and economic status, and family structure. For example, prior research has shown that the victims of identity theft are usually older than victims of property and violent crimes (DeLiema et al. 2021; Golladay and Holtfreter 2017). Other research suggests that females are more likely to become victims of identity theft than males (Allison et al. 2005; Anderson 2006). Many studies focused on examining the relationship between preventing identity theft and the likelihood of victimization. Using a sample collected from a large U.S. university, (Lai et al. 2012; Burnes et al. 2020) found that conventional coping (e.g., the shredding of bank statements) was effective in reducing identity theft occurrences.

In contrast, there are few studies investigating victim behaviors and/or characteristics in post-victimization along with capable guardianship. For instance, Reyns and Randa (2017) found that victims were more likely to contact LEAs for crimes characterized as serious when compared with those defined as less serious. Although their study addressed several questions related to victim reporting behaviors following identity theft victimization, it was limited to exploring the relationships between identity theft victims and capable guardians (i.e., LEAs and relevant financial institutions).

3. Current Study

Previous research has predominantly concentrated on the demographic characteristics of citizens and their online behaviors to predict instances of identity theft victimization, leaving a notable gap regarding the interaction between identity theft victims and capable guardians—specifically LEAs and other victim reporting agencies (Reyns and Randa 2017). This gap is significant due to the potential implications for the dynamics between capable guardians and victims. Historically, the CJ system has erroneously assumed that victims of crime are aware of these occurrences, and it acts accordingly (Muniz et al. 2024). This study examines why a reluctance to report identity theft victimization continues today (BJS 2023). Furthermore, we aim to explore the dynamics between guardians and victims, particularly focusing on victims' interactions with, and perceptions of, capable guardians following instances of identity theft. Additionally, this study highlights the pressing challenges associated with prosecuting identity theft cases.

4. Methods

This research was designed to elicit issues at two main levels: (1) victim interactions with capable guardians and (2) systemic factors such as legislation and response from LEAs. For victim interaction with capable guardians, the current study uses survey data on over 133,000 respondents drawn from the National Crime Victimization Survey Identity Theft Support (NCVS ITS) (BJS 2023). The NCVS is an ongoing self-report rotating panel survey designed to measure the extent and nature of criminal victimization within the United States. Data are collected semi-annually at 6 month intervals from a representative sample of residents aged 12 years and older, excluding persons residing in institutions (e.g., nursing homes and prisons), members of the military living in military barracks, and individuals who are crews of vessels. The response rate to the 2021 NCVS was 69.8%. Table 1 provides descriptive statistics for identity theft victimization as they were reported in the NCVS.

Table 1. Descriptive statistics for types of identity theft victimization.

	***N* (Total = 133,753)**	**Victims**	**%**	***Mean***	***SD***
Existing bank accounts	87,522	9037	10.3	1.90	0.30
Existing credit card accounts	75,503	12,232	16.2	1.84	0.36
Existing email or SMS accounts	77,244	4913	6.3	1.94	0.24

For systemic factors, this study explores existing PII legislation, major data breaches and assigned penalties, and challenges facing those in CJ to initiate legal actions involving identity theft (Kello 2021). Legislation related to protecting PII exists broadly at all levels of government globally and is regularly updated (ibid.).

Many identity theft crimes are never processed. The reasons for this include: jurisdictional issues, varying regulations related to identity theft crimes and prosecution, and insufficient personnel resources to address identity theft crimes. There is also an overwhelming reluctance of victims to file reports.

Legislation has been introduced in recent years making reporting by organizations of certain forms of cybercrimes mandatory. In Canada, this requirement was enacted with *Bill C-26*[1]—the *Critical Cyber Systems Protection Act* (CCSPA) (GOC 2022).

In the U.S., obligations to report data breaches are as follows:

> All 50 U.S. states plus Washington, D.C., and three federal territories have in place data breach notification laws, and the SEC has recently adopted a final rule requiring that, from 18 December 2023, public companies report material cybersecurity incidents in a Form 8-K within four business days from the date on which the incident was determined to be material. Smaller reporting entities have until June 2024 to comply. (ICLG 2023)

To date, no legislation exists to obligate individuals to report being victimized.

5. Results

Table 1 indicates that many respondents in the survey stated that they had experience(s) of identity theft victimization around 2021: 9037 victims for existing bank accounts misused, 12,232 victims for existing credit card accounts misused, and 4913 victims for existing email or SNS accounts misused.

5.1. Victim Interaction with Credit Bureau and/or Financial Institution

Table 2 reveals the respondents' behavior and interaction with the relevant credit bureau and/or financial institution. 68.3% of respondents indicated that they contacted someone at a credit card company or financial institution about misuse. In contrast, 10.3% of respondents indicated that they contacted a credit bureau. When respondents contacted a credit bureau, many individuals took initiative-taking actions such as requesting a credit report (57.7%), placing a fraud alert on their credit reports (66.9%), and/or freezing their credit report (56%). Importantly, 56.4% of respondents stated that they were very satisfied with the credit bureau's response and 24.2% of respondents stated that they were somewhat satisfied with the credit bureau's response.

Table 2. Victim interaction with a relevant financial institution.

Variables/Items	Response	Frequency (%)
Did you contact someone at a credit card company or financial institution about misuse?	Yes	6187 (68.3%)
	No	2855 (31.5%)
Did you contact a credit bureau?	Yes	637 (10.3%)
	No	5531 (89.3%)
When you contacted a credit bureau did you: request credit report?	Yes	376 (57.7%)
	No	259 (39.7%)
When you contacted a credit bureau did you: request corrections to your credit report?	Yes	234 (35.9%)
	No	396 (60.7%)
When you contacted a credit bureau did you: place a fraud alert on your credit report?	Yes	436 (66.9%)
	No	160 (24.5%)
When you contacted a credit bureau did you: place a freeze on your credit report?	Yes	365 (56.0%)
	No	262 (40.2%)
How satisfied were you with the credit bureau's response?	Very satisfied	368 (56.4%)
	Somewhat satisfied	158 (24.2%)
	Somewhat dissatisfied	27 (4.1%)
	Very dissatisfied	45 (6.9%)

5.2. Victim Interaction with Law Enforcement

This section elaborates on the characteristics of victims' interactions with LEAs.

Table 3 indicates that only 6.6% of respondents contacted LEAs. Overall, many respondents perceived LEAs' response to an identity theft incident to be satisfactory. Interestingly, 35% of respondents stated they were very satisfied with a LEA's response and 28% of respondents stated they were somewhat satisfied with a LEA's response. Among those who expressed dissatisfaction with a LEA's response, 51% of these respondents attributed their dissatisfaction to a strong belief that the LEA either did not or could not take any action.

Table 4 outlines the reasons why respondents opted not to reach out to a LEA. Of note, 45% of respondents reported that their issue was resolved by a credit card company, financial institution, or another organization, leading them to decide against contacting a LEA. Consequently, individuals who have engaged with their credit card company, banking institution, or other relevant entities for resolution might perceive no further need to involve LEAs. Approximately 15% of the respondents chose not to reach out to a LEA, reasoning that the issue was trivial or that they handled it on their own.

Table 3. Victim interaction with law enforcement.

Variables/Items	Response	Frequency (%)
Did you contact any law enforcement agencies?	Yes	596 (6.6%)
	No	8444 (93.2%)
Did the law enforcement agency take a police report?	Yes	428 (70.4%)
	No	162 (26.6%)
Did you get a copy of the police report?	Yes	224 (50.6%)
	No	192 (43.3%)
How satisfied were you with the law enforcement agency's response?	Very satisfied	213 (35.0%)
	Somewhat satisfied	171 (28.1%)
	Somewhat dissatisfied	72 (11.8%)
	Very dissatisfied	104 (17.1%)
Why were you dissatisfied: the police didn't or couldn't do anything?	Yes	98 (51.3%)
	No	78 (40.8%)
Why were you dissatisfied: the police only filled out a report?	Yes	30 (15.7%)
	No	146 (76.4%)
Why were you dissatisfied: the police said the crime did not fall in their jurisdiction?	Yes	16 (8.4%)
	No	160 (83.8%)
Why were you dissatisfied: the police gave me no information on what I should do about the crime?	Yes	20 (10.5%)
	No	156 (81.7%)
Why were you dissatisfied: the police never got back in contact with me/never learned outcome?	Yes	42 (22.0%)
	No	134 (70.2%)
Why were you dissatisfied: didn't feel my concerns/complaints were taken seriously?	Yes	41 (21.5%)
	No	135 (70.7%)
Why were you dissatisfied: the police were unable to catch the offender?	Yes	15 (7.9%)
	No	161 (84.3%)

Table 4. Reasons victim(s) decided not to contact a LEA.

Variables/Items	Response	Frequency (%)
Why did you decide not to contact a law enforcement agency: didn't know that I could report it?	Yes	794 (9.4%)
	No	7632 (90.2%)
Why did you decide not to contact a law enforcement agency: didn't think about reporting it?	Yes	887 (10.5%)
	No	7539 (89.1%)
Why did you decide not to contact a law enforcement agency: didn't know what agency was responsible for identity theft crimes?	Yes	216 (2.6%)
	No	8210 (97.0%)
Why did you decide not to contact a law enforcement agency: I didn't lose any money?	Yes	1339 (15.8%)
	No	7087 (83.7%)
Why did you decide not to contact a law enforcement agency: not important enough to report/small loss?	Yes	930 (11.0%)
	No	7496 (88.6%)
Why did you decide not to contact a law enforcement agency: took care of it myself?	Yes	1433 (16.9%)
	No	6993 (82.6%)
Why did you decide not to contact a law enforcement agency: credit card company/bank/other organization took care of problem?	Yes	3805 (45.0%)
	No	4621 (54.6%)
Why did you decide not to contact a law enforcement agency: didn't think the police would do anything?	Yes	920 (10.9%)
	No	7506 (88.7%)
Why did you decide not to contact a law enforcement agency: didn't want to bother the police?	Yes	129 (1.5%)
	No	8297 (98.0%)
Why did you decide not to contact a law enforcement agency: didn't find out until long after it happened?	Yes	22 (0.3%)
	No	8404 (99.3%)
Why did you decide not to contact a law enforcement agency: couldn't identify the offender?	Yes	410 (4.8%)
	No	8016 (94.7%)
Why did you decide not to contact a law enforcement agency: identity theft occurred in another state or outside of the U.S.?	Yes	128 (1.5%)
	No	8298 (98.0%)

5.3. A Brief Overview of PII Legislation and Related Industry Standards

Efforts have been undertaken by governments to enact legislation to assist those in CJ to act in cases of identity theft. In 1998, President Clinton signed into law the *Identity*

Theft and Assumption Deterrence Act (ITADA) to address the harm that could occur to those whose PII was stolen for the purpose of causing harm, specifically as it related to credit card and loan fraud, or other illegal purposes (US Senate 1998). An important component of ITADA is a means of identification with regard to someone's identity. Examples include: birth date, government-issued identification, and unique biological information such as fingerprints and other biometric identifiers (White and Fisher 2008). ITADA also defines fines and incarceration periods to be considered by the courts.

In addition to the ITADA, crimes involving identity theft may violate other statutes in the U.S.:

> Schemes to commit identity theft or fraud may also involve violations of other statutes such as identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344). Each of these federal offenses are felonies that carry substantial penalties—in some cases, as high as 30 years' imprisonment, fines, and criminal forfeiture. (DOJ 2024)

Two years later, the U.S. Senate held a hearing entitled, "ID Theft: When Bad Things Happen To Your Good Name" (US Senate 2000). During the question period, one Senator addressed the laborious task victims must endure if their PII has been stolen, and the numerous forms, calls, visits, and time required to report the theft, and to recover from any resulting harm, suggesting one form should be designed which could be used for these purposes (ibid.). The onus and procedures for victims continue to be costly, time-consuming, and onerous (FTC 2013; FTC 2024a, 2024b; State of California DOJ 2024).

The *Fair Credit Billing Act* (FTC 1974) and *Fair Credit Reporting Act* (FTC 2023b) provide victims in the United States with certain forms of protection in attempts to undo damage suffered if victimized by identity theft. Numerous other websites and offices exist in the US for victims to report PII crimes, as previously mentioned.

The *Better Cybercrime Metrics Act* introduced by Senator Schatz passed by the US Senate and approved in by the U.S. House of Representatives in March 2022, provides LEAs and legislators improved tools related to cyber threats and cybercrimes in the U.S. (Schatz 2022).

In the U.S., there are currently three main federal privacy acts: the *Health Insurance Portability and Accountability Act* (HIPPA), the *Children's Online Privacy Protection Act* (COPPA), and the *Privacy Act* of 1974. In addition, California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, and Delaware have enacted their own PII legislation (Bloomberg Law 2023).

Canada's privacy laws are outlined by the Office of the Privacy Commissioner under the *Privacy Act* (OPC 2019) and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) (OPC 2023). Canada's *Criminal Code* (R.S.C., 1985, c. C-46, s. 402.2 and s. 403) defines the crime of identity theft, issues related to trafficking of PII, and lists indictable offenses related to crimes involving identity theft (GOC 2024b). The Code was amended in 2010 to make identity fraud and identity theft criminal offenses (OPC 2017). Additionally, each province and territory in Canada has its own OPC that addresses identity theft and encourages reporting by victims.

Identity theft and the protection of PII are equally important in other areas of the world. As of 2023, according to the United Nations Conference on Trade and Development (UNCTAD), 71 percent of countries have some form of PII protection legislation in place, nine percent have draft legislation, and 15 percent have no existing legislation related to the protection of PII (UNCTAD 2023).

Europe implemented the *General Data Protection Regulation* (GDPR) in 2016 as a privacy and human rights law. It applies to all member states of the European Union (EU) and countries in the European Economic Area (EEA). Organizations outside of the EU zone that processes the PII of citizens or residents of the EU must also comply with GDPR legislation (GDPR 2024).

Industry has also provided standards for best practices to protect stored data. The *Payment Card Industry Data Security Standard* (PCI DSS) was established by the financial

industry as a standard requiring "how credit card companies, merchants, and payment processors handle sensitive cardholder information" (IBM 2023).

The U.S.-based National Institute of Standards and Technology (NIST) is widely recognized as the gold standard for providing standards and procedures related to technology. Their publication, "NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management, Version 1.0 is the result of a "collaborative effort between NIST and organizational and individual stakeholders in the public and private sectors" to provide guidance to build effective privacy risk into portfolios containing personal and sensitive data (NIST 2020).

The International Organizations for Standardization (ISO) developed three standards related to protecting data: ISO 27018—guidelines for protecting personal data stored in the cloud (Nir 2023; ISO 2019); ISO 27040—how to protect stored data, including stored data in the cloud (Nir 2023; ISO 2024); and ISO 27799—protecting personal health information (PHI) (Nir 2023; ISO 2016).

Educational institutions, private organizations, and LEAs continue to publish information on how to reduce having one's PII stolen, and how to address being victimized, and protective measures to take if made aware that a person's PII has been compromised (American Bar Association 2020; FTC 2013; Harvard University Police Department 2024; Office of Justice Programs 2011; USAGov 2024).

For those who elect to report an identity theft crime, there are a number of organizations in the U.S. they can contact for assistance, such as: LEAs; FTC (2013); Identity Theft Resources Center (ITRC 2024), Internal Revenue Service (IRS 2024), National Center for Victims of Crime (NCVC 2023), Office for Victims of Crime (OVC 2010), credit bureaus Equifax (Equifax 2024), TransUnion (TransUnion 2024), and local LEAs. Victims can also report identity theft and receive a detailed recovery plan from the FTC by accessing IdentityTheft.gov (FTC 2024a, 2024c).

Canadian resources for reporting identity theft crimes include: LEAs; the Canadian Anti-Fraud Centre (CAFC 2024), the Canadian Centre for Cybersecurity (GOC 2024a); and the RCMP's National Cybercrime Coordination Centre (NC3) (RCMP 2024). Various credit monitoring agencies are available to report crimes involving PII, such as TransUnion and Equifax, as examples.

5.4. Review of Major Data Breaches and Assigned Penalties

The frequency of major data breaches or violations continues to escalate globally as cybercriminals find new ways to infiltrate large quantities of data at rest stored on legacy systems, or in the cloud. Major data breaches continue to escalate, as cybercriminals become increasingly proficient at circumventing protective measures to prevent exfiltration or interception of collected, stored, or transmitted PII.

Based on the number of users impacted, records exposed, or affected accounts, the 15 largest data breaches of the 21st century include: Yahoo (2013), three billion accounts; Alibaba (2018), over one billion accounts; LinkedIn (2021), 700 million users; Sina Weibo (2020), 538 million accounts; Facebook (2019), 533 million users; Marriott International (Starwood) (2018), 500 million customers; Yahoo (2014), 500 million accounts; Adult Friend Finder (2016), 412 million accounts; MySpace (2013), 360 million user accounts; NetEase (2015), 235 million user accounts; Court Ventures (Experian) (2013), 200 million accounts; LinkedIn (2012), 165 million users; Dubsmash (2018), 162 million user accounts; and Adobe (2013), 152 million user accounts—a cumulative total of over five billion user accounts (Hill and Swinhoe 2022).

Europe's GDPR rules, introduced in 2018, include severe penalties for companies who do not sufficiently protect the PII they collect. In 2020, fines were issued to Google (€7M) and H&M (€35M). In 2021, fines were issued against META (€746M), Amazon (€746M), TikTok (€750M), and WhatsApp (€225M). GDPR issued subsequent fines in 2023 against META (€1.2B), and TikTok (€12.7M) (Exabeam 2024).

Reported data compromises and numbers of records exposed from 2005 to 2023 in the United States alone increased from 157 to 67 million records to 3205 compromises and 353 million records respectively (Petrosyan 2024). Healthcare, financial services, and manufacturing represented the top three industry sectors for data breaches in 2022 (Madnick 2024).

It is reported that T-Mobile has suffered eight data breaches since 2019—two occurring in 2023, with 37 million customer's PII being stolen in January, and 836 customers having their PII accessed in April (Humphries 2023). Three different cybercriminal groups claimed collectively that they hacked US communications giant T-Mobile over 100 times in SIM-swapping cyber-intrusions (AT&T and Verizon have also been targets, but to a smaller degree) (Krebson Security 2023).

Shockingly, reputational damage for organizations that suffer major data breaches or violations for not adequately protecting PII and other customer data at rest has not proven to be long-lasting. People continue to willingly share their PII with organizations where PII has been previously stolen, even in cases where companies have been hacked repeatedly. According to T-Mobile's own reports, they "[delivered] record customer growth, adding an expected industry-best 6.4 million postpaid customers and 2.0 million broadband customers in 2022" (T-Mobile 2023).

Other concerns pertaining to breaches of information security relate to the frequency that such threats occur in multinational financial institutions, such as the case of Morgan Stanley (Mahle et al. 2017). This prominent global financial services entity has been subjected to substantial civil penalties as a consequence of its continuous shortcomings in upholding robust practices for information security. Spanning an eight-year timeframe from 2015 to 2023, the company was implicated in multiple significant security breaches that underscored persistent weaknesses in safeguarding sensitive information (C. Page 2021).

According to Trend Micro (2015), the sequence of breaches commenced with an incident unfolding between 2011 and 2014, during which a former staff member illicitly gained access to and transferred data from around 730,000 accounts to his personal server, subsequently compromised by cybercriminals (U.S. Securities and Exchange Commission 2016). Later, in January 2015, an employee named Galen Marsh pilfered and subsequently disclosed online the personal information of 350,000 clients (The Heritage Foundation 2015; Moore 2015). Additionally, according to C. Page (2022), between 2015 and 2019, the organization encountered further scrutiny for inadequate disposal of hardware containing the personal details of 15 million customers. The stolen PII was subsequently found to be sold online.

In 2016, Morgan Stanley faced two new incidents. Initially, complications arose when a vendor subcontracted to erase data from decommissioned devices and engaged an unauthorized party, resulting in several devices retaining unencrypted personal data. The second incident in the same year, involved a software vulnerability that left unencrypted data remnants on devices that were not duly inventoried following decommissioning. Furthermore, 42 servers potentially housing unencrypted customer information were reported missing (Stempel 2022).

Morgan Stanley confirmed another breach in 2021 involving the pilferage of personal data from its clients due to a breach into the Accellion FTA server utilized by a third-party vendor (Kiesel et al. 2022). This breach, occurring in December 2020, led to the exposure of clients' addresses and Social Security numbers (Picus Security 2022). It is important to note that despite the encryption of files, the hackers successfully acquired the decryption key as well (C. Page 2021).

In reaction to these breaches, Morgan Stanley came under regulatory scrutiny. On 16 November 2023, two principal legal entities, the Florida Office of the Attorney General and the New York State Office of the Attorney General, concluded a settlement agreement with Morgan Stanley. The firm agreed to pay $6.5 million in response to its inadequacies in safeguarding customer data, following a thorough investigation into these security lapses (Florida Office of the Attorney General 2023; New York State Office of the Attorney General 2023).

As evidenced by the occurrences in Table 5, data breaches can remain undetected for extended periods of time, but for those that are discovered and successfully prosecuted, significant financial penalties have been successfully levied.

Table 5. Largest global data breaches or violations.

Organization	Location	Violation/ Data Breach	Date(s) Occurred	Data Compromised	Number of Victims	Penalties ($US)
Didi Global	China	Violation	Began 2015	A-facial recognition data, B-records location data, C-other data	A-107M, B-167M, C-Unknown	$1.9B
Amazon	Europe	Breach of the GDPR	2021	(Alleged) violation of cookie consent	10,000	$877M (proposed fine)
Equifax	United States	Data Breach	2017		150M	$575M
Instagram	United States	Violation	2022	Data related to minors	Unknown	$403M
TikTok	Ireland	Violation	2023	Violating children's data privacy	Unknown	$370M
T-Mobile	United States	Data Breach	2021	Customer data	77M	$350M
Meta (Facebook)	Ireland	Violation	2022	Compromise of users' PII	500M	$277M
WhatsApp	Ireland	Violation	2018–2021	Cross-border data protection infringements	Unknown	$255M
Home Depot	United States	Data Breach	2014	A-Credit card, B-email info.	A-50M, B-53M	$200M
Capital One	United States	Data Breach	2019	Various forms of PII	100M	$190M
Uber	United States	Data Breach	2016	Various forms of PII	600K drivers, 57M user accounts	$148M
Morgan Stanley	United States	Data Breach	2020	Various forms of PII of current and former clients	15M	$120M
Google Ireland	Ireland	Violation	2021	Cookie consent	Unknown	$102M

Sources: Hill and Sharma (2024); Soo (2022).

5.5. Challenges Facing Those in CJ to Initiate Legal Actions Involving Identity Theft

Stolen PII is regularly uploaded to the Dark Web where it can remain indefinitely, often by those intending to use it for fraudulent purposes or make it available for purchase by others (Liu et al. 2021). It is imperative that everyone involved in CJ understands that once PII is posted on the Dark Web, the risk of being victimized for those whose PII has been compromised will exist into perpetuity.

Challenges related to successfully initiating and processing cases of identity theft can seem insurmountable and not worthy of the time, effort, or costs to initiate investigations or legal proceedings. One major challenge is that laws related to conventional crimes are not necessarily applicable to cybercrimes due to the uniqueness of how and where cybercrimes are committed (Koops 2012). Numerous other issues impact effective investigations of identity theft crimes. These include, but are not limited to:

Differences in federal and state identity theft laws can complicate multi-jurisdictional crimes (Arnell and Faturoti 2023; Kello 2021; Perl 2004);

Collection of digital evidence requires specific procedures, that if not followed correctly, can invalidate the evidence and jeopardize any criminal proceedings (NIST 2022);

Lack of multi-country cooperation during investigations (Arnell and Faturoti 2023; Peters and Jordon 2019);

LEA's limitations (financial and personnel) to acquire and train personnel to respond to and effectively investigate cases of identity theft (CPKN 2021; Maloney et al. 2022; Sarkar and Shukla 2023);

Lengthy and costly investigative and legal processes; and

The ability of cybercriminals to mask their identification (Acton 2024; Guccione 2024; Volle 2024).

One overriding factor impacting decisions to process identity theft crimes is proving in a court of law precisely when and where PII was acquired and associating that information with a specific crime (Carson and Cameron 2023; Macnab 2022; Gelowitz et al. 2021). This restrictive mindset will do little to improve how identity theft crimes can be more effectively addressed, given the greater concern that once acquired, PII can exist on the Dark Web into perpetuity and be used for illicit purposes.

A 2024 report by cybersecurity experts at SecurityDiscovery.com found a data pool on the Dark Web of over 26 billion data breach records containing over 12TB (terabytes) of data acquired from past data breaches, including Chinese tech giant Tencent, LinkedIn, Deezer, Adobe, Canva, and numerous adult sites, including 220 million records from AdultFinder (Snyder 2024). These vast amounts of PII can be utilized forever to commit fraud.

Other challenges relate to crimes involving PII that exist on the Dark Web. Although electronic evidence is admissible, guaranteeing the accuracy and authenticity of evidence must be carried out according to strict guidelines. Timestamp information can be difficult to establish. Varying privacy laws globally can inhibit requests to obtain warrants. Lack of cooperation by companies storing data, such as Meta and Google, regularly complicates legal requests for historical electronic information. These and other factors can contribute to the complexities of identifying who committed identity fraud to produce successful legal actions (Lach 2014).

Other issues complicate initiating criminal actions in PII-related crimes. LEA officers may not be equipped to determine actual or potential future losses when someone reports having their PII stolen, leading them to believe that filing a report is sufficient. Lawyers, cognizant of the extensive time and costs and uncertain outcomes related to initiating a lawsuit for a single or small group of individuals, may determine initiating legal proceedings are unwarranted. Attempts to initiate class actions against those who possess vast quantities of data at rest pertaining to customers, members, or others that is breached can be difficult to initiate, if the decision for certification is based primarily on proving potential risk of victimization into the future (Gelowitz et al. 2021).

Determining future victimization as a result of PII theft and misuse can be difficult to measure (Burnes et al. 2020). As we have acknowledged, predicting how or when stolen PII may be used illicitly, and determining when and where it was acquired and by whom, can be extremely challenging. However, this should not be a sufficient reason not to initiate actions to pursue those who commit identity theft-based crimes.

By example, a proposed class action in Setoguchi v Uber related to a successful data breach of Uber that occurred in Canada was rejected by the Court of Queen's Bench in Alberta based on the following opinion: "As there was no evidence the hacker had used anyone's personal information, Associate Chief Justice John Rooke found there was no tangible harm, merely speculation that there might be loss or harm in the future" (Gelowitz et al. 2021). Such decisions ignore the present and future risks for those whose PII is stolen.

Addressing these challenges will help reduce victimization rates and provide greater protection from significant and ongoing harm for those whose PII has been or may be used to compromise their lives at some point in time.

6. Discussion

Our research and analysis highlight an immediate need for increased rates of investigation and prosecution for identity theft-based crimes. This is primarily based on data that suggest when someone's PII is compromised, the possibility they will become a victim of an identity theft crime at some time is realistic, given the longevity of availability of PII once posted on the Dark Web (Li et al. 2019). Based on our analysis and findings, we urge those in CJ to consider the findings in this paper when determining whether to proceed with identity theft investigations and prosecutions. This is equally applicable to applications for class actions involving the theft of PII.

Private, public, and government organizations are increasingly requesting, or requiring individuals to provide PII for various purposes, thereby ultimately inheriting the

responsibility to safeguard that information once in their possession. Individuals also freely share their PII while utilizing the Internet, through online purchases, queries, and when using social media websites. The exponential increase in sharing PII is increasingly providing criminals with information that can be used against individuals to commit fraud, particularly if posted on the Dark Web.

Many who are made aware they have been victimized by an identity theft-based crime do contact LEA to file reports, but as our research revealed, a greater number elect not to contact authorities about being victimized based on their assumption that investigation and prosecution of those committing the crime is unlikely to occur (BJS 2023). Unfortunately for identity theft victims, initiating investigations or legal proceedings for crimes involving PII can be complicated (ibid.).

Reasons include: a lack of awareness of the potential suffering that can ensue (Mandelblit 2001; Schmitz 2008; Harrell and Thompson 2023b); a lack of training in how to investigate these types of crimes (Lach 2014); outdated legislation that does not address advancements in identity theft crimes, particularly as it pertains to the Internet and stored data (Perl 2004); and complexities related to how different jurisdictions categorize and address identity theft crimes (Dixon 2019; Kello 2021).

Historically, two issues contribute to a reluctance to investigate and prosecute identity theft crimes. First, the requirement to prove when and where the PII was acquired and by whom. Second, the opinion that if no crime has occurred against someone whose PII has been stolen, there is no way to establish that person may be harmed in the future by identity fraud.

As we demonstrated, the amount of PII being acquired by nefarious characters is continuing to increase to levels never previously experienced. This can be attributed to an exponential rise in those using the Internet, increasing amounts of stored PII being required by organizations and governments, and an increasing number of successful cyber intrusions. Once acquired, it is regularly posted for sale on the Dark Web to commit identity theft-based crimes (Liu et al. 2021).

We identified some successful prosecutions against those responsible for safeguarding PII that were compromised. However, these cases represent a minimal number of effective investigations and prosecutions, compared to the number of data breaches that occur. Even for companies successfully prosecuted for failing to adequately protect PII data at rest, some continued to experience additional data breaches. This suggests they did not take proactive measures to improve their security measures, and that penalties for a previous data breach were not deemed sufficiently impactive to result in better security, policies, and procedures to be adopted to prevent additional cyber intrusions from occurring (Humphries 2023; Krebson Security 2023; C. Page 2021; Stempel 2022).

The fines we highlighted against organizations found guilty of data breaches are paltry in comparison to their market capitalization and revenue streams. Repeat offending by some may suggest that pursuing organizations for not adequately protecting PII can be ineffective, time consuming, expensive, and not worth the effort. This would not be a correct assumption. As greater amounts of data continue to acquire and stored by private, public, and government organizations, the need for improved legislation of how PII data are protected must occur to support efforts to investigate, prosecute and fine those who fail to adequately protect such valued data. This is a core aspect of facilitating class actions against those who fail to adequately protect entrusted data at rest containing PII.

Throughout this paper, we highlighted that potential victimization and suffering from identity theft are sufficient justifications for a consideration to proceed with criminal actions against those who steal PII or fail to adequately protect stored data from being acquired through illegal means.

In order for this to occur, three conditions must exist. First, incidents involving illicitly obtained PII must be reported to the appropriate authorities. One study revealed that only seven percent of those victimized by an identity theft crime filed a report to a LEA (Harrell 2019). People must become more confident that reporting identity theft will not be

a futile process, and trust that LEA, prosecutors, judges, and governments will investigate and initiate criminal proceedings involving identity theft. As evidenced in our analysis of NCVS data related to reporting of identity theft to authorities and financial institutions, there continues to be a reluctance of victims of identity theft to report being victimized through identity theft (BJS 2023).

Second, that users of technology and those involved in CJ are made more aware that the consequences for victims of identity theft can be life-changing—potentially requiring weeks, months or years to rectify damages suffered from illegal use of their PII (FTC 2011; Harrell and Thompson 2023b; Macnab 2022; Mandelblit 2001; Schmitz 2008; Stein 2023).

Third, courts must become more amenable to certifying class actions against organizations that fail to adequately protect against the infiltration of stored PII that has been entrusted to them, particularly with regard to organizations who store an individual's health or financial information (Kello 2021).

The real and potential financial and personal costs that can be experienced by those who PII is compromised and used to commit fraud against them can be devastating. As rates of victimization continue to escalate, it is important that those involved in CJ take a more proactive approach to addressing any and all legal methods to investigate, pursue, arrest, charge, and prosecute those involved in identity theft crimes. While offering our suggestions of how to approach this objective, we acknowledge additional research in the area of identity theft crimes and their potential to cause life-changing damages to victims is required to reduce victimization rates of identity theft.

Policy Implications

1. Reporting and trust building: encouraging victims and potential victims to report incidents of identity theft is critical. This requires a concerted effort to build trust between the public and LEA, prosecutors, judges, and governments. Many existing programs that provide valuable information about identity theft, best practices to avoid becoming a victim, and what to do if victimized (FTC 2023c; OPC 2024a). Policy changes could include creating more accessible and user-friendly reporting mechanisms, along with public awareness campaigns highlighting the importance of reporting and the supportive measures in place to protect and assist victims. This approach could mitigate the reluctance to report incidents, as shown by our analysis of the NCVS data. For instance, Van der Meulen (2006) demonstrated that public awareness campaigns in the U.S., U.K., and the Netherlands offered significant benefits. Firstly, by equipping the public with knowledge about identity theft, individuals are better positioned to prevent it, potentially decreasing the crime's prevalence. Secondly, when identity theft does occur, public awareness initiatives provide victims with tools to seek timely assistance through the appropriate channels, facilitating their recovery process.
2. Law enforcement training and resources: there is a need for specialized training for CJ personnel on the complexities of identity theft and the illicit acquisition of PII (Koziarski and Lee 2020; Maloney et al. 2022), if clearance rates for identity theft crimes are to improve (Vieraitis and Shuraydi 2015). This includes enhancing digital forensic capabilities and understanding the intricacies of the Dark Web where stolen PII is traded (Maloney et al. 2022). Policies could focus on allocating more resources towards training programs, equipment, and the recruitment of experts in cybercrimes to bolster investigative and prosecutorial capacities (Robertson 2019).
3. Legal and regulatory frameworks: the research underscores the necessity for harmonized legal frameworks and standards for PII protection and the handling of digital evidence (Koziarski and Lee 2020). Policy implications might involve revising privacy laws to facilitate cross-jurisdictional cooperation and streamlining the processes for obtaining warrants for digital evidence (Newman and McNally 2005). There is also a call for policies that encourage or mandate companies to cooperate with LEA in providing historical electronic information when investigating identity theft (RCMP 2013).

4. Victim support and remediation: the persistent vulnerability of identity theft victims calls for robust policies focused on long-term support and remediation. These measures should provide victims with easy access to correct inaccurate credit reports or address fraudulent financial activities. Legislative efforts must prioritize establishing streamlined mechanisms for victims to swiftly rectify such issues and recover from financial losses. Identity fraudsters, who possess ample time and technical expertise, exploit system loopholes, making post-crime support for victims essential in any identity crime prevention framework (Fazely 2020). While most victims are reimbursed by banks or commercial organizations, there are still those who do not receive such protection. The emotional distress and inconvenience caused by identity theft often surpass the financial losses. Thus, an effective support system should go beyond simple reimbursement—it must ensure immediate financial relief from pre-established funds.
5. Enhancing prosecutorial practices: the difficulty in proving the acquisition and misuse of PII in court suggests a need for evolving prosecutorial strategies and legal standards (International Centre for Criminal Law Reform and Criminal Justice Policy 2011). Policy recommendations might include the development of new legal doctrines or evidentiary rules that acknowledge the unique challenges of prosecuting cybercrimes, especially those involving identity theft (Washington State Department of Commerce 2019).
6. Class action facilitation: for breaches involving large volumes of compromised PII, the research suggests policies that make it easier to certify class-action lawsuits against entities that fail to protect data adequately is in need of immediate attention (Carson and Cameron 2023; Macnab 2022; Gelowitz et al. 2021). This particularly applies to organizations holding sensitive health records, credit records, or financial information. Existing Legislations need to evolve to incentivize organizations to adopt more stringent data protection measures to avoid potential class-action litigation.

7. Conclusions

Previous research related to identity theft has predominantly concentrated on the demographic characteristics of citizens and their online behaviors in efforts to predict instances of identity theft victimization. What has not been extensively examined is why victims remain reluctant to report being victimized. We determined that a major contributor to this reluctance is a belief by victims that those involved in CJ have historically not provided sufficient solutions to encourage victims to file reports. In addition, we examined many challenges faced by those in CJ to better address identity theft crimes, and suggest that updates to current legislation, or new legislation could provide more effective ways to process identity theft crimes. We also provided additional insight into the consequences identity theft victims experience, particularly if their PII is posted on the Dark Web, and how these threats can exist into perpetuity. We propose that if rates of victimization from identity theft-based crimes are to decline, reporting of victimization must increase, and that those charged with initiating legal procedures against anyone involved in the theft or failure to protect PII, or fraudulent use of such data, could be more effective if they were better equipped to do so. Our findings support the need to raise awareness for UoT and those entrusted with storing PII, since protecting information related to someone's identity is of the utmost importance. Equally, it is essential to understand that once PII is made available on the Dark Web, the question of whether someone may become a victim of identity theft in the future is not if, but when.

The current study acknowledges limitations in predicting when PII that is acquired for illicit purposes may be used for fraudulent purposes, and ongoing challenges to identify the perpetrators. Future research is essential to deepen the understanding of how PII is distributed and utilized on the Dark Web, and to explore innovative methods for tracking and prosecuting identity theft crimes more effectively. Additionally, further studies could investigate the psychological and social impacts of identity theft on victims to form more

comprehensive support systems. Expanding upon these findings will be crucial as the digital economy continues to grow, and the collection of PII becomes even more pervasive.

Author Contributions: Conceptualization, C.S.K., S.B. and M.M.T.-A.; methodology, C.S.K., S.B. and M.M.T.-A.; formal analysis, C.S.K., S.B. and M.M.T.-A.; investigation, C.S.K., S.B. and M.M.T.-A.; resources, C.S.K., S.B. and M.M.T.-A.; data curation, C.S.K., S.B. and M.M.T.-A.; writing, C.S.K., S.B. and M.M.T.-A.; project, C.S.K., S.B. and M.M.T.-A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data supporting the findings of this study are available from the authors upon reasonable request.

Conflicts of Interest: Christopher S. Kayser was employed by the Cybercrime Analytics Inc. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

ABS. 2024. Personal Fraud. Statistics About Personal Fraud, Including Card Fraud, Identity Theft, and Scams (Phishing, Romance, Computer Support, Financial Advice and More). Australian Bureau of Statistics. Available online: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release (accessed on 24 August 2024).

Acton, Brian. 2024. The Origins and History of the Dark Web. Available online: https://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/ (accessed on 7 June 2024).

Akin, Jim. 2024. U.S. Fraud and Identity Theft Losses Topped $10 Billion in 2023. Experian. Available online: https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ (accessed on 7 September 2024).

Allison, Stuart F. H. 2003. "A Case Study of Identity Theft". USF Tampa Graduate Theses and Dissertations. Available online: https://digitalcommons.usf.edu/etd/1322 (accessed on 7 June 2024).

Allison, Stuart F. H., Arnie M. Schuck, and Kim M. Lersch. 2005. Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice* 33: 19–29. [CrossRef]

American Bar Association. 2020. Identity Theft and Fraud: How to Evaluate and Manage Risks. Available online: https://www.americanbar.org/news/abanews/publications/youraba/2020/youraba-march-2020/identity-theft-and-fraud/ (accessed on 7 June 2024).

Anderson, Keith B. 2006. Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing* 25: 160–71.

Anderson, Keith B., Erik Durbin, and Michael A. Salinger. 2008. Identity Theft. *Journal of Economic Perspectives* 22: 171–92. [CrossRef]

Arnell, Paul, and Bukola Faturoti. 2023. The prosecution of cybercrime—Why transnational and extraterritorial jurisdiction should be resisted. *International Review of Law, Computers and Technology* 37: 29–51. [CrossRef]

AVtest. 2023. Malware. Available online: https://www.av-test.org/en/statistics/malware/ (accessed on 7 June 2024).

Balaji. 2018. Hackers Selling More Than 200 Million Stolen Data from Chinese Hotel Chain in Dark Web. GBHackers on Security. Available online: https://gbhackers.com/hackers-selling-stolen-data/ (accessed on 7 June 2024).

Basheer, Randa, and Bassel Alkhatib. 2021. Threat from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence. *Journal of Computer Networks and Communications* 2021: 1302999. [CrossRef]

Beckman, Jeff. 2023. A Look at Key Dark Web Statistics (2023 Data Update). TechReport. Available online: https://techreport.com/statistics/dark-web-statistics/ (accessed on 7 June 2024).

Beshiri, Arber S., and Arsim Susuri. 2019. Dark Web and its Impact on Online Anonymity and Privacy: A Critical Analysis and Review. *Journal of Computer and Communications* 7: 30–43. [CrossRef]

BJS. 2022. Identity Theft and Financial Fraud. Available online: https://bjs.ojp.gov/topics/crime/identity-theft (accessed on 7 June 2024).

BJS. 2023. Victims of Identity Theft, 2021. Available online: https://bjs.ojp.gov/document/vit21.pdf (accessed on 7 June 2024).

Bloomberg Law. 2023. Consumer Data Privacy Laws. Everything You Need to Know About Consumer Data Privacy Laws So You Can Mitigate Risk and Stay Compliant. Available online: https://pro.bloomberglaw.com/consumer-data-privacy-laws/#:~:text=California%20led%20the%20charge%20in,went%20into%20effect%20on%20Jan (accessed on 7 June 2024).

Burnes, David, Marguerite DeLiema, and Lynn Langton. 2020. Risk and Protective Factors of Identity Theft Victimization in the United States. *Preventive Medicine Reports* 17: 101058. [CrossRef] [PubMed]

CAFC. 2024. Canadian Anti-Fraud Centre. Available online: https://antifraudcentre-centreantifraude.ca/index-eng.htm (accessed on 4 September 2024).

California Legislative Information. 2023. California Penal Code Part 1, Title 13, Chapter 8, Section 530.5. Available online: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=530.5#:~:text=(a)%20Every%20person%20who%20willfully,medical%20information%20without%20the%20consent (accessed on 14 October 2024).
Carson, Robert, and Simon Cameron. 2023. Canadian Privacy Class Actions Evolve Beyond Traditional Data Breaches. Osler. Available online: https://www.osler.com/en/insights/updates/canadian-privacy-class-actions-evolve-beyond-traditional-data-breaches/ (accessed on 13 October 2024).
Chen, George. 2023. Beyond detection: Uncovering unknown threats. *Cyber Security: A Peer-Reviewed Journal* 7: 6–15.
Choi, Kyung-shick. 2011. *Cyber Criminology. Exploring Internet Crimes and Criminal Behavior*, 1st ed. New York: Routledge. [CrossRef]
Cohen, Lawrence E., and Marcus Felson. 1979. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44: 588–608. [CrossRef]
Copes, Heith, Kent R. Kerley, Rodney Huff, and John Kane. 2010. Differentiating identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice* 38: 1045–52. Available online: https://www.uab.edu/cas/thecenter/images/Documents/Differentiating-identity-theft-An-exploratory-study-of-victims-using-a-national.pdf (accessed on 7 June 2024). [CrossRef]
CPKN. 2021. Policing in a Digital World: Competencies and Training for Canadian Law Enforcement. Canadian Police Knowledge Network. Available online: https://www.cpkn.ca/en/news/competency-based-management-framework-for-digital-competencies-in-canadian-policing/ (accessed on 7 September 2024).
DeLiema, Marguerite, David Burnes, and Lynn Langton. 2021. The Financial and Psychological Impact of Identity Theft Among Older Adults. *Innovation in Aging* 5: igab043. [CrossRef] [PubMed]
DiNardi, Gaetano. 2023. 14 Dangers of Identity Theft That Can Leave You Reeling. AURA. Available online: https://www.aura.com/learn/dangers-of-identity-theft#:~:text=9.-,You%20could%20experience%20psychological%20harm%20and%20emotional%20distress,task%20of%20repairing%20the%20damage (accessed on 7 June 2024).
Dixon, William. 2019. Fighting Cybercrime—What Happens to the Law When the Law Cannot Be Enforced. World Economic Forum. Available online: https://www.weforum.org/agenda/2019/02/fighting-cybercrime-what-happens-to-the-law-when-the-law-cannot-be-enforced/ (accessed on 22 August 2024).
DOJ. 2023. In 2021, 1 in 10 Persons Had Been Victims of Identity Theft in the Past 12 Months. Available online: https://bjs.ojp.gov/document/vit21_pr.pdf (accessed on 25 August 2024).
DOJ. 2024. Identity Theft. Criminal Division. Available online: https://www.justice.gov/criminal/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (accessed on 4 September 2024).
Equifax. 2024. Don't Let Identity Theft Catch You off Guard. Available online: https://www.equifax.com/personal/identity-theft-protection/ (accessed on 1 November 2024).
Exabeam. 2024. GDPR Fines Structure and the Biggest GDPR Fines to Date. Available online: https://www.exabeam.com/explainers/gdpr-compliance/gdpr-fines-structure-and-the-biggest-gdpr-fines-to-date/ (accessed on 25 August 2024).
Fazely, Aida. 2020. Identity Crimes in the UK: An Examination of the Strategies Employed by Front-Line Practitioners in the Public and Private Sector to Detect, Prevent and Mitigate Against This Crime. Ph.D. dissertation, Middlesex University, London, UK.
FBI. 2017. Darknet Takedown. Authorities Shutter Online Criminal Market AlphaBay. In *FBI News*; July 20. Available online: https://www.fbi.gov/news/stories/alphabay-takedown (accessed on 7 June 2024).
FBI. 2022. Internet Crime Report. 2022. [PDF]. Available online: https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf (accessed on 7 June 2024).
FBI. n.d. History. Ross William Ulbright's Laptop. Available online: https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop#:~:text=Ross%20William%20Ulbricht.-,Known%20online%20as%20Dread%20Pirate%20Roberts,%20Ulbricht%20ran%20a%20darknet,to%20conceal%20its%20users%E2%80%99%20locations (accessed on 7 June 2024).
Finklea, Kristin. 2014. Identity Theft: Trends and Issues. Congressional Research Service. Available online: https://sgp.fas.org/crs/misc/R40599.pdf (accessed on 7 June 2024).
Florida Office of the Attorney General. 2023. Morgan Stanley AVC Florida. Available online: https://www.myfloridalegal.com/sites/default/files/2023-11/executed-morgan-stanley-avc-florida.pdf (accessed on 7 June 2024).
FTC. 1974. Fair Credit Billing Act. 15 U.S.C. 1666-1666j. Available online: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-billing-act (accessed on 7 June 2024).
FTC. 2004. FTC Issues Final Rules on FACTA Identity Theft Definitions, Active Duty Alert Duration, and Appropriate Proof of Identity. Available online: https://www.ftc.gov/news-events/news/press-releases/2004/10/ftc-issues-final-rules-facta-identity-theft-definitions-active-duty-alert-duration-appropriate-proof (accessed on 20 August 2024).
FTC. 2011. Medical Identity Theft. FAQ's for Health Care Providers and Health Plans. Available online: https://www.ftc.gov/business-guidance/resources/medical-identity-theft-faqs-health-care-providers-health-plans (accessed on 7 June 2024).
FTC. 2013. Taking Charge. What to Do If Your Identity Theft Is Stolen? [PDF]. Available online: https://www.justice.gov/usao-wdmi/file/764151/ (accessed on 7 June 2024).
FTC. 2023a. Consumer Sentinel Network Data Book 2022. Top Three Reported Identity Thefts by Year. Available online: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf (accessed on 7 June 2024).
FTC. 2023b. Fair Credit Reporting Act. Available online: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act (accessed on 7 June 2024).

FTC. 2023c. Identity Theft Awareness Week. Available online: https://consumer.ftc.gov/consumer-alerts/2023/01/identity-theft-awareness-week-events-focus-how-reduce-your-risk (accessed on 13 October 2024).
FTC. 2024a. Deter-Detect-Defend. [PDF]. Available online: https://www.justice.gov/usao-edpa/file/763696/dl (accessed on 7 June 2024).
FTC. 2024b. Recovering from Identity Theft. Available online: https://consumer.gov/scams-identity-theft/recovering-identity-theft#what-it-is (accessed on 7 June 2024).
FTC. 2024c. Report Identity Theft and Get a Recovery Plan. Available online: https://www.identitytheft.gov/ (accessed on 7 September 2024).
Gelowitz, Mark A., Robert Carson, W. David Rankin, Emily Mackinnon, Legranre Harper, and Celine Lauren. 2021. Canadian Courts Confirm Significant Limits on Privacy Class Actions. Osler. Available online: https://www.osler.com/en/insights/updates/canadian-courts-confirm-significant-limits-on-privacy-class-actions/ (accessed on 13 October 2024).
GDPR. 2024. Complete Guide to GDPR Compliance. Available online: https://gdpr.eu/ (accessed on 7 June 2024).
GOC. 2022. Bill C-26: An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts. Available online: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html (accessed on 6 September 2024).
GOC. 2024a. Canadian Centre for Cyber Security. Government of Canada. Available online: https://www.cyber.gc.ca/en (accessed on 4 September 2024).
GOC. 2024b. Criminal Code R.S.C., 1985, c. C-46. Government of Canada. Justice Laws Website. Available online: https://laws-lois.justice.gc.ca/eng/acts/c-46/section-402.2.html (accessed on 4 September 2024).
Golladay, Katelyn, and Kristy Holtfreter. 2017. The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims Offenders* 12: 741–60. [CrossRef]
Guccione, Darren. 2024. What Is the Dark Web? How to Access It and What You'll Find. CSO. Available online: https://www.csoonline.com/article/564313/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (accessed on 7 June 2024).
Guedes, Ines, Margarida Martins, and Carla S. Cardoso. 2023. Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal* 36: 472–97. [CrossRef]
Harnett, Cindy. 2024. Stolen London Drugs Data Posted Online in Ransomware Attack. Times Colonist. Available online: https://www.timescolonist.com/local-news/stolen-london-drugs-data-posted-online-in-cyberattack-8811654 (accessed on 7 June 2024).
Harrell, Erika. 2019. *Victims of Identity Theft, 2016*; 1-29/NCJ 251147. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics. Available online: https://www.bjs.gov/content/pub/pdf/vit16.pdf (accessed on 7 June 2024).
Harrell, Erika, and Alexandra Thompson. 2023a. Victims of Identity Theft, 2021. Bureau of Justice Statistics. Available online: https://bjs.ojp.gov/library/publications/victims-identity-theft-2021 (accessed on 7 June 2024).
Harrell, Erika, and Alexandra Thompson. 2023b. Victims of Identity Theft, 2021. U.S. DOJ. BJS. Available online: https://bjs.ojp.gov/document/vit21.pdf (accessed on 11 September 2024).
Harvard University Police Department. 2024. Identity Theft. Available online: https://www.hupd.harvard.edu/identity-theft#:~:text=Identity%20thieves%20use%20this%20information,rating%20and%20denial%20of%20credit (accessed on 7 June 2024).
Hill, Michael, and Dan Swinhoe. 2022. The 15 Biggest Data Breaches of the 21st Century. CSO. Available online: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html (accessed on 7 June 2024).
Hill, Michael, and Shweta Sharma. 2024. The Biggest Data Breach Fines, Penalties, and Settlements so Far. CSO. Available online: https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html (accessed on 7 June 2024).
Hoar, Sean B. 2001. Identity Theft: The Crime of the New Millennium. U.S. Department of Justice. USA Bulletin. Available online: https://www.hsdl.org/?view&did=439991 (accessed on 7 June 2024).
Humphries, Matthew. 2023. It's Only May, but T-Mobile Has Already Been Hacked Twice This Year. PCMag. Available online: https://www.pcmag.com/news/its-only-may-but-t-mobile-has-already-been-hacked-twice (accessed on 7 June 2024).
IBM. 2023. What Is Personally Identifiable Information (PII)? Available online: https://www.ibm.com/topics/pii (accessed on 7 June 2024).
ICLG. 2023. Cybersecurity Laws and Regulations USA 2024. Available online: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa (accessed on 6 September 2024).
Identity Theft Resource Center (ITRC). 2023a. 2022 Consumer Impact Report. Experian. Available online: https://www.idtheftcenter.org/wp-content/uploads/2023/03/2022-Consumer-Impact-Report_V4.1_2023-Update.pdf (accessed on 7 June 2024).
Identity Theft Resource Center (ITRC). 2023b. 2022 Data Breach Report. [PDF]. Available online: https://www.idtheftcenter.org/publication/2022-data-breach-report/ (accessed on 7 June 2024).
Identity Theft Resouce Center (ITRC). 2024. Your Life, Your Identity. Let's Keep It That Way. Available online: https://www.idtheftcenter.org/ (accessed on 1 November 2024).
Identitytheft.org. 2024. 2024 Identity Theft Facts and Statistics. Available online: https://identitytheft.org/statistics/#:~:text=33%2525%2520of%2520Americans%2520Faced%2520Some,theft%2520attempt%2520in%2520their%2520lives (accessed on 11 September 2024).

Insurance Information Institute. 2024. Fats + Statistics: Identity Theft and Cybercrime. Available online: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (accessed on 24 August 2024).
International Centre for Criminal Law Reform and Criminal Justice Policy. 2011. Responding to Victims of Identity Theft: A Manual for Law Enforcement Agents, Prosecutors and Policy Makers. Available online: https://icclr.org/wp-content/uploads/2019/06/00-Victims-of-Identity-Crime-Manual.pdf?x21689 (accessed on 13 October 2024).
IRS. 2024. Identity Theft Central. Available online: https://www.irs.gov/identity-theft-central (accessed on 1 November 2024).
Irvin-Erickson, Yasemin. 2024. Identity fraud victimization: A critical review of the literature of the past two decades. *Crime Science* 13: 2024. [CrossRef]
ISO. 2016. ISO 27779:2016. Health Informatics—Information Security Management in Health Using ISO/IEC 27002. Available online: https://www.iso.org/standard/62777.html (accessed on 1 November 2024).
ISO. 2019. ISO/IEC 27018:2019. Information Technology—Security Techniques—Code of Practice for Protection of Personlly Identifiable Information (PII) in Public Clouds Acting as PII Processors. Available online: https://www.iso.org/standard/76559.html (accessed on 1 November 2024).
ISO. 2024. ISO/IEC 27040:2024(en). Information Technology—Security Techniques—Storage Security. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:27040:ed-2:v1:en (accessed on 1 November 2024).
Jones, Todd. 2023a. The 12 Latest Types of Social Engineering Attacks 2024. Aura. Available online: https://www.aura.com/learn/types-of-social-engineering-attacks (accessed on 5 October 2024).
Jones, Todd. 2023b. What is Synthetic Identity Theft? (And How To Protect Yourself). AURA. Available online: https://www.aura.com/learn/synthetic-identity-theft-fraud (accessed on 7 June 2024).
Jovanovic, Bojan. 2023. A Not-So-Common Cold: Malware Statistics in 2023. DataProt. Available online: https://dataprot.net/statistics/malware-statistics/ (accessed on 7 June 2023).
Kastner, Erika. 2020. History of the Dark Web [Timeline]. SOS. Available online: https://www.soscanhelp.com/blog/history-of-the-dark-web (accessed on 7 June 2024).
Kayser, Christopher S. 2020. *Cybercrime Through Social Engineering—The New Global Crisis*. Calgary: Cybercrime Analytics Inc.
Kayser, Christopher S., Mary E. Mastrorilli, and Robert Cadigan. 2020. Preventing cybercrime: A framework for understanding the role of human vulnerabilities. *Cyber Security: A Peer-Reviewed Journal* 3: 159–74. [CrossRef]
Kello, Lucas. 2021. Cyber legalism: Why it fails and what to do about it. *Journal of Cybersecurity* 7: tyab014. [CrossRef]
Kiesel, Karl, Tom Deep, Austin Flaherty, and Suman Bhunia. 2022. Analyzing multi-vector ransomware attack on Accellion file transfer appliance server. Paper presented at the 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Bol and Split, Croatia, July 5–8; Piscataway: IEEE, pp. 1–6.
Koops, Bert-Jaap. 2012. Criminal law and Cyberspace as a Challenge for Legal Research. *SCRIPTed* 9: 354. Available online: https://script-ed.org/article/criminal-law-cyberspace-challenge-legal-research/ (accessed on 22 August 2024). [CrossRef]
Koops, Bert-Jaap, and Ronald E. Leenes. 2006. Identity theft, identity fraud and or identity-related crime. *Datenschutz und Datensicherheit—DuD* 30: 553–56. [CrossRef]
Koziarski, Jacek, and Jin R. Lee. 2020. Connecting Evidence-Based Policing and Cybercrime. *Policing: An International Journal* 43: 198–211. Available online: https://www.crimrxiv.com/pub/go7thxn6/release/1 (accessed on 12 October 2024). [CrossRef]
Krebson Security. 2023. Hackers Claimed They Breached T-Mobile More Than 100 Times. Available online: https://krebsonsecurity.com/2023/02/hackers-claim-they-breached-t-mobile-more-than-100-times-in-2022/ (accessed on 7 June 2024).
Lach, Arkadiusz. 2014. The Problems of Investigating Identity Theft in SNS. Paper presented at the International Conference on Cyber-Crime Investigation and Cyber Security, Kuala Lumpur, Malaysia, November 17–19; Available online: https://www.academia.edu/9346566/The_Problems_of_Investigation_of_Identity_Theft_in_SNS (accessed on 7 June 2024).
Lai, Fujun, Dahui Li, and Chang-Tseh Hsieh. 2012. Fighting identity theft: The coping perspective. *Decision Support Systems* 52: 353–63. [CrossRef]
Leukfeldt, Erik R., and Majid Yar. 2016. Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior* 37: 263–80. [CrossRef]
Li, Yuan, Adel Yazdanmehr, Jingguo Wang, and H. Raghav Rao. 2019. Responding to identity theft: A victimization perspective. *Decision Support Systems* 121: 13–24. [CrossRef]
Liu, Haun, Kai Li, Yan Chen, and Xin (Robert) Luo. 2023. Is personally identifiable information really more valuable? Evidence from consumers' willingness-to-accept valuation of their privacy information. *Decision Support Systems* 173: 114010. Available online: https://www.sciencedirect.com/science/article/abs/pii/S0167923623000854 (accessed on 7 June 2024). [CrossRef]
Liu, Yizhi, Fang U. Lin, Zara Ahmed-Post, Mohammedreza Ebrahimi, Ning Zhang, James L. Hu, Jingyu Xin, Weifeng Li, and Chen Hsinchun. 2021. Identifying, Collecting, and Monitoring Personally Identifiable Information: From the Dark Web to the Surface Web. Available online: https://par.nsf.gov/servlets/purl/10218332 (accessed on 7 June 2024).
Macnab, Aidan. 2022. Privacy Class Actions 2021: More Misuse-of-Information Claims, Certification Used as a Screening Tool. Canadian Lawyer. Available online: https://www.canadianlawyermag.com/practice-areas/privacy-and-data/privacy-class-actions-2021-more-misuse-of-information-claims-certification-used-as-screening-tool/363558#:~:text=An%20uptick%20in%20misuse-of,the%20internet%20and%20digital%20technology (accessed on 13 October 2024).
Madnick, Stuart. 2024. Why Data Breaches Spiked in 2023. Harvard Business Review. Available online: https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (accessed on 7 June 2024).

Mahle, J. D., N. Colvin, and E. S. Cyr. 2017. Government Enforcement When Private Date Information Is Breached: Guidance and Best Practices. *N. Ky. L. Rev.* 44: 41. Available online: https://scholar.google.com/scholar?hl=es&as_sdt=0,14&q=in+Government+Enforcement+When+Private+Date+Information+Is+Breached:+Guidance+and+Best+Practices;+Mahle,+Jacob+D.;+Colvin,+Nathan;+Cyr,+Emily+St.&btnG= (accessed on 7 June 2024).

Maloney, Christopher J., N. Prabah Unnithan, and Weiqi Zhang. 2022. Assessing Law Enforcement's Cybercrime Capacity and Capability. ARTICLES. Available online: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- (accessed on 7 September 2024).

Mandelblit, Bruce. 2001. Identity Theft: A New Security Challenge. Security. Available online: https://www.securitymagazine.com/articles/77638-identity-theft-a-new-security-challenge-1 (accessed on 7 June 2024).

Martin, Craig. 2019. [Pulse] Lenders, You've Got Hurdles to Overcome on the Path Toward the Digital Mortgage. Housingwire. Available online: https://www.housingwire.com/articles/48129-pulse-lenders-youve-got-hurdles-to-overcome-on-the-path-toward-the-digital-mortgage/ (accessed on 7 June 2024).

McCants, Cassidy, and Sean Golanka. 2024. U.S. Identity Theft Statistics 2024. Available online: https://www.consumeraffairs.com/finance/identity-theft-statistics.html (accessed on 24 August 2024).

Moore, Michael J. 2015. Morgan Stanley Fires Worker Accused of Stealing Client Data. Bloomberg Business. Available online: https://www.bloomberg.com/news/articles/2015-01-05/morgan-stanley-fires-employee-accused-of-stealing-client-data (accessed on 7 June 2024).

Muniz, Caitlyn N., Taylor Fisher, Katelyn Smith, Roan Ali, C. Jordan Howell, and David Maimon. 2024. Hello, You've been hacked: A study of victim notification preferences. *Journal of Crime and Justice*, 1–17. [CrossRef]

NCVC. 2023. Victim Recovery Checklist. FINRA Investor Education Foundation. Available online: https://victimsofcrime.org/victim-recovery-checklist/ (accessed on 7 June 2024).

New York State Office of the Attorney General. 2023. Attorney General James and Multistate Coalition Secure $6.5 Million from Morgan Stanley for Failing to Protect Customer Data. Available online: https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-65-million-morgan-stanley (accessed on 7 June 2024).

Newman, Greame R., and Megan M. McNally. 2005. Identity Theft Literature Review. Available online: https://www.ojp.gov/pdffiles1/nij/grants/210459.pdf (accessed on 7 June 2024).

Ng, Alfred. 2017. Buyers, Sellers and Cops on the Hunt for AlphaBay's Successor. CNET. Available online: https://www.cnet.com/news/privacy/alphabay-hansa-silk-road-dream-market-dark-web-shuts-down/ (accessed on 7 June 2024).

Nir, Onn. 2023. The Complete List of Data Security Standards. Reflectiz. Available online: https://www.reflectiz.com/blog/data-security-standards/ (accessed on 7 September 2024).

NIST. 2020. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf (accessed on 4 September 2024).

NIST. 2022. NIST Interagency Report NIST IR 8387. Digital Evidence Preservation. Considerations for Evidence Handlers. Available online: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf (accessed on 7 September 2024).

Office of Justice Programs. 2011. OJP Fact Sheet. Identity Theft. Available online: https://www.ojp.gov/sites/g/files/xyckuh241/files/archives/factsheets/ojpfs_idtheft.html (accessed on 7 June 2024).

Oliver, Gannicus. 2024. What Is the Dark Web? How to Access It Safely? PrivacySavvy. Available online: https://privacysavvy.com/security/safe-browsing/dark-web-safety (accessed on 21 August 2024).

OPC. 2017. Identity Theft and You. Office of the Privacy Commissioner. Available online: https://www.priv.gc.ca/media/2034/guide_idt_e.pdf (accessed on 4 September 2024).

OPC. 2019. The Privacy Act. Office of the Privacy Commissioner. Available online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/ (accessed on 4 September 2024).

OPC. 2023. The Personal Information Protection and Electronic Documents Act (PIPEDA). Office of the Privacy Commissioner. Available online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/ (accessed on 7 June 2024).

OPC. 2024a. Identity Theft and You. Available online: https://www.priv.gc.ca/en/privacy-topics/identities/identity-theft/guide_idt/%E2%80%AF (accessed on 13 October 2024).

OPC. 2024b. 2023–2024 Survey of Canadian Businesses on Privacy-Related Issues. Office of the Privacy Commissioner. Available online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2024/por_2023-24_bus/ (accessed on 23 August 2024).

OVC. 2010. Expanding Services to Reach Victims of Identity Theft and Financial Fraud. Victim Assistance: Lessons from the Field. Publication Date: October 2010. NCJ 230590. Available online: https://ovc.ojp.gov/sites/g/files/xyckuh226/files/pubs/ID_theft/stepsforvictims.html (accessed on 7 June 2024).

Page, Carly. 2021. The Accellion Data Breach Continues to Get Messier. TechCrunch. Available online: https://techcrunch.com/2021/07/08/the-accellion-data-breach-continues-to-get-messier/ (accessed on 7 June 2024).

Page, Carly. 2022. Morgan Stanley Hard Drives Data Breach. TechCrunch. Available online: https://techcrunch.com/2022/09/21/morgan-stanley-hard-drives-data-breach/?guccounter=1 (accessed on 7 June 2024).

Page, Rosalyn. 2023. 10 Things You Should Know About Navigating the Dark Web. CSO. Available online: https://www.csoonline.com/article/566577/10-things-you-should-know-about-dark-web-websites.html (accessed on 7 June 2024).

Perl, Michael W. 2004. It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft. *The Journal of Criminal Law and Criminology* 94: 169–208. [CrossRef]
Peters, Allison, and Amy Jordon. 2019. Countering the cyber enforcement gap: Strengthening global capacity on cybercrime. *Journal of National Security Law & Policy* 10: 487.
Petrosyan, Ani. 2024. Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023. Statista. Available online: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (accessed on 7 June 2024).
PEW Research Center. 2019. Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information. Available online: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (accessed on 23 August 2024).
Picus Security. 2022. Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022. Available online: https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (accessed on 7 June 2024).
Raman, Raghu, Vinith K. Nair, Prema Nedungadi, Indrakshi Ray, and Krishnashree Achuthan. 2023. Darkweb research: Past Achuthan, present, and future trends and mapping to sustainable development goals. *Heliyon* 9: e22269. Available online: https://www.sciencedirect.com/science/article/pii/S240584402309477X (accessed on 7 June 2024). [CrossRef]
Randa, Ryan, and Bradford W. Reyns. 2020. The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior* 41: 1290–304. [CrossRef]
Ravichandran, Hari. 2023. My Social Security Number Was Found on the Dark Web. Help! AURA. Available online: https://www.aura.com/learn/social-security-number-found-on-dark-web (accessed on 7 June 2024).
RCMP. 2013. National Identity Theft Crime Strategy For a Stronger and Safer Canada. Available online: https://publications.gc.ca/collections/collection_2013/grc-rcmp/PS64-105-2013-eng.pdf (accessed on 13 October 2024).
RCMP. 2024. RCMP Specialized Unit Combats Cybercrime Through Teamwork. Gazette Magazine. Available online: https://grc.ca/en/gazette/rcmp-specialized-unit-combats-cybercrime-through-teamwork (accessed on 4 September 2024).
Reflectiz. 2024. Deep Dive into the Black Market of PII. Available online: https://www.reflectiz.com/blog/pii-black-market/ (accessed on 7 June 2024).
Reyns, Bradford W., and Ryan Randa. 2017. Victim reporting behaviors following identity theft victimization: Results from the National Crime Victimization Survey. *Crime & Delinquency* 63: 814–38.
Robertson, James. 2019. The Impact of the Digital Society on Police Recruit Training in Canada. Available online: https://dam-oclc.bac-lac.gc.ca/download?is_thesis=1&oclc_number=1344012535&id=1e56137e-1c79-4395-8099-df7b1243b479&fileName=Robertson_James_G.pdf (accessed on 12 October 2024).
Rubenking, Neil J. 2022. 5 Ways Identity Theft Can Ruin Your Life. Available online: https://www.pcmag.com/how-to/5-ways-identity-theft-can-ruin-your-life (accessed on 7 June 2024).
Sarkar, Gargi, and Sandeep K. Shukla. 2023. Behavioural analysis of cybercrime: Paving the way for effective policing strategies. *Journal of Economic Criminology* 2: 100034. [CrossRef]
Schatz, Brian. 2022. Schatz Legislation To Help Fight Cybercrime Signed Into Law. Available online: https://www.schatz.senate.gov/news/press-releases/schatz-legislation-to-help-fight-cybercrime-signed-into-law (accessed on 20 August 2024).
Schmitz, Cristin. 2008. Identity Theft Victim Claims Emotional Distress. Available online: https://www.law.com/almID/4dcafacd160ba0ad5700106d/?slreturn=20240009141617 (accessed on 7 June 2024).
Seitz, Lyndon. 2024. Key Internet Statistics in 2024 (Including Mobile). Broadband Search. Available online: https://www.broadbandsearch.net/blog/internet-statistics (accessed on 7 June 2024).
Sharp, Tracy, Andrea Shreve-Neiger, John Kane, William Fremouw, and Shawn Hutton. 2004. Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences* 49: 1–6. [CrossRef]
Shinder, Debra L. 2011. What Makes Cybercrime Laws so Difficult to Enforce? Tech Republic. Available online: https://www.techrepublic.com/article/what-makes-cybercrime-laws-so-difficult-to-enforce/ (accessed on 22 August 2024).
Sky News. 2024. Ticketmaster Hit by Cyber Attack—With Hackers 'Offering to Sell Customer Data on Dark Web'. Available online: https://uk.news.yahoo.com/ticketmaster-hit-cyber-attack-hackers%20123700937.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAMRv6FGKSzQ_knnlhm7NuUWiUvnCfCsL3oDCV3CGDxq_gCWOJ5v4BRa7D0kEQ70dWRxdPEUpqBcCzB5lxFuHgpqWUdfPduTNOLnG7qBsTXLFtOJl_Ts8mFnJ-BHLq9Zu6h0alux7j-gx7Ewk3qQ9mRe1ivtuKGenbViFZMf2JEhO (accessed on 7 June 2024).
Snyder, Brady. 2024. Massive Data Breach Includes 26 Billion Records and 12 TB of Data. Android Headlines. Available online: https://www.androidheadlines.com/2024/01/massive-data-breach-includes-26-billion-records-and-12tb-of-data.html/amp (accessed on 7 June 2024).
Soo, Zen. 2022. China's Didi Global Fined $1.2 Billion for Data Violations. AP. Available online: https://apnews.com/article/technology-china-data-privacy-cheng-wei-d7c76a253e50d5b5aa8218eb1d3cebbd (accessed on 7 June 2024).
State of California DOJ. 2024. Identity Theft Victim Checklist. Rob Bonta. Attorney General. Available online: https://oag.ca.gov/idtheft/facts/victim-checklist (accessed on 7 June 2024).
Statista. 2023. Number of Internet and Social Media Users Worldwide as of October 2023. Available online: https://www.statista.com/statistics/617136/digital-population-worldwide/ (accessed on 7 June 2024).

Statista. 2024. Rates of Identity Thefts in Canada from 2012 to 2013. Available online: https://www.statista.com/statistics/544904/identity-theft-rate-canada/ (accessed on 24 August 2024).
Stein, Josh. 2023. Medical Identity Theft. North Carolina Department of Justice. Attorney General's Office. Available online: https://ncdoj.gov/protecting-consumers/protecting-your-identity/medical-identity-theft/ (accessed on 7 June 2024).
Stempel, Jonathan. 2022. Morgan Stanley to Pay $60 Million over Data Breaches. Yahoo Finance. Available online: https://ca.finance.yahoo.com/news/morgan-stanley-pay-60-million-165325091.html (accessed on 7 June 2024).
The Heritage Foundation. 2015. Cyber-Attacks on U.S. Companies Since November 2014. Available online: https://www.heritage.org/cybersecurity/report/cyber-attacks-us-companies-november-2014 (accessed on 7 June 2024).
T-Mobile. 2023. T-Mobile Delivers Record Customer Growth, Adding an Expected Industry-Best 6.4 Million Postpaid Customers and 2.0 Million Broadband Customers in 2022. Available online: https://www.t-mobile.com/news/business/t-mobile-preliminary-customer-results-2022 (accessed on 7 June 2024).
TransUnion. 2024. What Is Identity Theft? Available online: https://www.transunion.ca/identity-theft (accessed on 1 November 2024).
Trend Micro. 2015. The Morgan Stanley Breach: Understanding the Nature of Insider Threats. Available online: https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/the-morgan-stanley-breach-nature-of-insider-threats (accessed on 7 June 2024).
Trend Micro. 2018. Stolen Data from Chinese Hotel Chain Sold in Deep Web. Available online: https://www.trendmicro.com/en_us/research/18/i/we-uncovered-personally-identifiable-information-pii-stolen-from-a-china-based-hotel-chain-being-sold-on-a-deep-web-forum-we-were-monitoring.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Anti-MalwareBlog+(Trendlabs+Security+Intelligence+Blog) (accessed on 7 June 2024).
U.S. Securities and Exchange Commission. 2016. SEC: Morgan Stanley Failed to Safeguard Customer Data. Available online: https://www.sec.gov/news/press-release/2016-112 (accessed on 7 June 2024).
UNCTAD. 2023. Data Protection and Privacy Legislation Worldwide. United Nations Conference on Trade and Development. Available online: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed on 7 June 2024).
US Senate. 1998. S. Rept. 105-274—The Identity Theft and Assumption Deterrence Act. congress.gov. Available online: https://www.congress.gov/congressional-report/105th-congress/senate-report/274/1 (accessed on 7 June 2024).
US Senate. 2000. S. Hrg. 106-885—ID Theft: When BAD Things Happen to Your Good Name. GovInfo. Available online: https://www.govinfo.gov/app/details/CHRG-106shrg69821/context (accessed on 7 June 2024).
USAGov. 2024. Identity Theft. Available online: https://www.usa.gov (accessed on 7 June 2024).
Van der Meulen, Nicole. 2006. *The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the European Union*. Report Commissioned by the National Infrastructure Cyber Crime Program (NICC). Available online: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=7dddefbe7a6751f11fe0e8baf66a982d69999035 (accessed on 1 November 2024).
Veltman, Chloe. 2024. Millions of Customers' Data Found on Dark Web in Latest AT&T Data Breach. NPR. Available online: https://www.npr.org/2024/03/30/1241863710/att-data-breach-dark-web (accessed on 7 June 2024).
Vieraitis, Lynne M., and Amny Shuraydi. 2015. Identity Theft. In *Oxford Handbook Topics in Criminology and Criminal Justice*, 2012 online ed. Oxford: Oxford Academic. Available online: https://academic.oup.com/edited-volume/41333/chapter/352358022 (accessed on 12 October 2024). [CrossRef]
Volle, Adam. 2024. Dark Web Science & Tech. Available online: https://www.britannica.com/topic/dark-web (accessed on 7 June 2024).
Washington State Department of Commerce. 2019. Financial Fraud and Identity Theft Investigation and Prosecution Program. Progress Report on Task Force and Recommendations Pursuant to RCW 43.330.300(1)(c). Available online: https://www.commerce.wa.gov/wp-content/uploads/2020/06/2019-Financial-Fraud-Identify-Theft-Report.pdf (accessed on 13 October 2024).
White, Michael D., and Christopher Fisher. 2008. Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review* 19: 3–24. [CrossRef]
Whitty, Monica T., and Tom Buchanan. 2012. The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking* 15: 181–83. Available online: https://core.ac.uk/reader/74227018?utm_source=linkout (accessed on 7 June 2024). [CrossRef]
Williams, Matthew L. 2015. Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe and the Country and Individual Level. *The British Journal of Criminology* 56: 21–48. [CrossRef]
Zolton, Miklos. 2023. Dark Web Price Index 2023. Privacy Affairs. Available online: https://www.privacyaffairs.com/dark-web-price-index-2023/ (accessed on 7 June 2024).