European Journal of Social Sciences Studies
ISSN: 2501-8590
ISSN-L: 2501-8590
Available on-line at: www.oapub.org/soc

DOI: 10.46827/ejsss.v12i1.2161 Volume 12 | Issue 1 | 2026

STOLEN LIVES: STORIES OF VICTIMS OF IDENTITY THEFT

Dianne Chlaire V. Duron[1i],
Rowela Cartin-Pecson[2]
[1]Faculty of the College of Criminal Justice Education,
University of Mindanao,
Davao City, Philippines
[2]Professor,
College of Criminal Justice Education,
University of Mindanao,
Davao City, Philippines

Abstract:
This study examined the lived experiences of identity theft victims in Davao City as they navigated the consequences of the crime and coped to regain control over their digital and personal lives. Using a qualitative phenomenological design, the researcher conducted in-depth interviews with seven victims to capture the essence of their experiences. Thematic analysis revealed several major impacts of identity theft, including compromised accounts, heightened digital distrust, emotional and psychological distress, occupational disruptions, financial loss, and reputational damage. Recovery was influenced by multiple factors, such as support from family and friends, access to technical and professional assistance, spiritual grounding, and the successful retrieval of compromised digital accounts. Participants emphasized the importance of strengthening account security, exercising caution online, and maintaining consistent vigilance. The study underscores the need for more awareness campaigns, proactive security measures, and accessible government support systems to mitigate the harms of identity theft and to guide victims toward effective recovery and resilience.

Keywords: criminal justice, digital distrust, cybercrime, Davao City

1. Introduction

Identity theft is a pervasive and insidious crime that can have devastating consequences for its victims (Maillet, 2023). In their 2023 study, Harrel and Thompson reported that individuals aged 16 and above residing in the United States reported experiencing identity theft, according to the 2021 Identity Theft Supplement (ITS) accompanying the National Crime Victimization Survey (NCVS). Additionally, in 2021, approximately 23.9

[i] Correspondence: email dduron@umindanao.edu.ph

million individuals aged 16 or older were victims of identity theft in the preceding 12 months.

2. Literature Review

Among the identity theft incidents reported in 2021, some involved the misuse of a single type of existing account, such as a credit card or bank account. Identity theft victims incurred financial losses totaling $16.4 billion. Further, in the same year, there were reported cases of individuals aged 16 or older who experienced the unauthorized use of an existing email or social media account. However, in the Philippines, identity theft is also rapidly spreading as Filipinos are fond of using the Internet as a means of communication. During the closing week of March 2024, the PNP Anti-Cybercrime Group (PNP ACG) documented 225 cybercrime cases. This represents a 40.79% decrease from the previous week's count of 380 cases. The top five prevalent offenses among the reported incidents included 96 cases – Online Scams, 63 – Illegal Access, 18 – Identity Theft, 15 – Online Libel, and 8 – Online Threats. It was also said that the reduction in online activity, combined with individuals' proactive efforts, driven by heightened awareness and reinforced security measures, has played a significant role in the notable decrease in cybercrime cases observed during this timeframe (PNP AntiCybercrime Group Manila, 2024).

In the study by Balistoy *et al.* (2024), 41 cases of identity theft were reported in 2020. In 2021, only 18 cases were reported, compared to 2020, when there was a reduction of over half. Furthermore, the researcher was able to gather data from the PNP-ACG Davao, which also documented several reported cases of Identity Theft. In the year 2022, there were 5 cases. In 2023, it reached 58 cases, and in 2024, the number of events reached 137.

Additionally, in 2025, there were 129 reported cases of identity theft. Even with the decline in reported identity theft cases, it is imperative not to become complacent. In an era marked by swift technological advancements, perpetrators of identity theft are also adapting their tactics rapidly (Roser, 2023). The emotional toll of identity theft should not be overlooked, as victims often grapple with feelings of vulnerability, betrayal, and fear long after the initial incident (DeLiema *et al.*, 2021). However, despite efforts to combat identity theft through legislation, technology, and public awareness campaigns, the problem persists and continues to evolve. As criminals develop increasingly sophisticated techniques to commit identity theft, it is crucial to deepen our understanding of the personal consequences of this crime. Efforts should focus on creating effective solutions that address both the systemic and individual effects of identity theft. This includes addressing the emotional, financial, and societal impacts while also improving preventive measures and legal frameworks to protect individuals from these increasingly sophisticated threats (Tadros, 2011).

The importance of this research lies in delving into the stories of identity theft victims, which provides invaluable insights into the multifaceted nature of this crime and the urgent need for effective solutions (Hedayati, 2012). Resolving the issue of identity

theft is a critical endeavor with far-reaching implications for individuals, communities, and society at large (Ahmed, 2020). This research underscores the importance of resolving identity theft by highlighting its impact on fundamental rights, financial stability, emotional well-being, community trust, crime prevention, and legal compliance (Kayser *et al.*, 2024). Moreover, given the rampant cases of identity theft, this research seeks to illuminate the human dimension of identity theft, highlighting the urgent need for enhanced awareness, prevention strategies, and support for victims navigating the complex aftermath of such breaches.

The advent of the Internet has completely transformed our way of life. It has completely revamped how to communicate to the point where it has become our primary mode of everyday interaction. Furthermore, the Internet evolved beyond mere information exchange; it became a sophisticated, multifaceted instrument empowering individuals to generate content, connect, and even immerse themselves in alternate realities (Dentzel, 2024). Identity theft has already raised concerns, even amid the various crises. Advancements in technology have transformed the conventional crime of identity theft. Previously, information was gathered through methods like stealing mail, rifling through trash, or eavesdropping on public phone conversations. A skilled cybercriminal can now steal identities online by using hidden methods to collect personal information. They often target people who are unaware of the danger. These criminals use tricks such as phishing, fake websites, and malware to steal data without the victim realizing it, making it harder for individuals to protect themselves against these attacks (Neira, 2016).

This study is grounded in Routine Activity Theory (RAT), developed by Cohen and Felson in 1979. Routine Activity Theory (RAT) provides a framework for understanding victim vulnerability in identity theft cases. It suggests that crime occurs when motivated offenders encounter suitable targets lacking capable guardians. Although not probing offender motivations directly, RAT helps examine how victims' daily routines, online behaviors, and financial habits might make them susceptible to identity theft. By identifying weaknesses such as using unprotected public Wi-Fi or reusing passwords, the study aims to better understand victim vulnerability and inform preventive measures. However, RAT's focus on opportunity overlooks the emotional toll of identity theft, underscoring the need for a broader perspective for a comprehensive understanding. To further support the context of identity theft, this study is also anchored in the Human Identification Theory (HIT) developed by M. Lynn LoPucki. As technology becomes more integrated into daily life, individuals become increasingly vulnerable to cybercrime. It is imperative to safeguard sensitive information, such as one's mother's maiden name, passwords, and Social Security number. Additionally, maintaining the confidentiality of token-based identification further enhances individual security. Perpetrators also exploit biometric data, including unique physical identifiers such as fingerprints and retinal scans. Thieves gain access to others' credit records through methods such as scrutinizing IDs, intercepting emails, and orchestrating deceptive phone calls in which an impostor is involved. Once a thief obtains this information, they exploit it to their advantage (LoPucki, 2002).

3. Materials and Methods

This section describes the method the researcher used to carry out the study, including the study participants, materials, instruments, and the design and procedures.

3.1 Study Participants

In this study, the participants will be seven (7) victims of identity theft, all of legal age and residing in Davao City. As a result, participants were identified, and once identified, the researcher will send them formal letters outlining the study's nature and encouraging them to participate. As Creswell and Poth (2018) noted, center-based qualitative studies include a small range of participants, usually between 5 and 25, to make it possible to investigate the details of each participant.

For the sampling method, the researcher employed purposive sampling. This allowed the researcher to strategically select participants or cases that could provide rich, informative data for the study, especially those victims of identity theft who have shown exemplary improvement in their lives (Creswell, 2013).

In terms of inclusion, the subjects included in this study were individuals residing in Davao City who had personally experienced identity theft within the last five years. Participants were required to be at least 18 years old at the time of the incident and capable of providing informed consent and a clear account of their experience. All gender identities were represented, and the study welcomed a wide range of socio-demographic profiles, including variations in educational attainment, income level, marital status, religious affiliation, and ethnic background. Victims from all employment statuses, whether employed in the public or private sector, self-employed, unemployed, students, or retirees, were eligible to participate, allowing for a comprehensive understanding of how identity theft impacts people across different occupational and economic circumstances.

Exclusion criteria included individuals who did not reside in Davao City, those who had not personally experienced identity theft, minors under 18, and persons unable to provide reliable information due to cognitive limitations. In addition, institutional representatives who were not direct victims but had only secondhand knowledge of cases (such as law enforcement or bank personnel) were not considered part of the main participant group. However, they may have been consulted separately as key informants. Regarding withdrawal, participants may withdraw from the study at any time without providing a reason, and such withdrawal will not result in any penalty, loss of benefits, or adverse consequences. Upon withdrawal, all data previously provided by the participant, whether in written form, audio recordings, or transcripts, will be removed from the study and securely destroyed, unless explicit consent is given for its retention.

3.2 Profile of the Study Participants

Table 1 presents this study's seven (7) participants who were interviewed in depth under the codenames Trojan 1, Trojan 2, Trojan 3, Trojan 4, Trojan 5, Trojan 6, and Trojan 7. In terms of gender, six participants are female, and one participant is male. With respect to

age, one participant is 28 years old, one is 22 years old, two are 24 years old, one is 25 years old, one is 55 years old, and one is 26 years old. In terms of occupation, one participant is a teacher, one is a student, three are working students, one is unemployed, and one is employed in the call center industry. Thus, participants of this study answered the research questions through in-depth interviews to compile a thorough data set for the completion of this study.

Table 1: Profile of the Study Participants

Codename	Gender	Age	Occupation
Trojan 1	Female	28	Teacher
Trojan 2	Female	22	Student
Trojan 3	Male	24	Working Student
Trojan 4	Female	24	Working Student
Trojan 5	Female	25	Working Student
Trojan 6	Female	55	Unemployed
Trojan 7	Female	26	Call Center

3.3 Materials and Methods

For data collection, the researcher used an interview questionnaire with probing questions to elicit further details from the selected participants' responses. Using open-ended questions, participants will describe their lived experiences with identity theft, and their responses will be recorded and transcribed. Each participant will receive a hard copy of their transcribed interview for review, allowing them to modify or clarify their responses during the member-checking process to ensure accuracy and credibility.

Moreover, data collection will utilize a digital audio recorder to accurately capture participants' narratives, with prior consent obtained for recording. The recordings will be transcribed using reliable transcription software to ensure accuracy and completeness.

The instrument's validation process involved multiple steps to ensure reliability and accuracy. The interview guide was initially developed based on the research objectives and relevant literature. Then, it was submitted to a panel of internal and external validators for thorough review and validation using the following criteria: ethics, artistry, and rigor. The feedback from these experts was incorporated to refine the questions further. Finally, adjustments were made based on their feedback to finalize the interview guide.

3.4 Design and Procedure

This study employed a qualitative-phenomenological design. This was the most suitable method, as the study involved victims' personal experiences of identity theft. When the aim is to gain a comprehensive knowledge of participants' personal experiences, social circumstances, and interpretations of events, qualitative research is the best choice (Creswell & Poth, 2018). In the study of Tenny *et al.* (2022), a qualitative study represents a strong methodological paradigm designed to elicit a comprehensive understanding of human behavior and social contexts by prioritizing the underlying motivations and processes, specifically the how and why of a phenomenon, over numerical frequency.

Additionally, phenomenological research aims to uncover the common truth of an experience by listening to those who lived through it.

This method is a popular way to study human life because it helps researchers understand how people think and feel. By examining these personal stories, a researcher can learn more and discover the universal nature or core meaning of the event being studied (Qutoshi, 2018).

The researcher followed all necessary steps to ensure rigor and validity in conducting this study. First, the researcher submitted the interview guide to the validators. After thoroughly reviewing and validating it by a panel of internal and external evaluators, the researcher then complied with the UMERC requirements. Following this, the researcher requested an endorsement letter from the Dean of the Professional Schools, noted by my Research Adviser, addressed to the Regional Chief of the Anti-Cyber Crime Group Davao, to solicit data for the research participants.

After receiving consent, the researcher set up in-person interviews. Seven (7) victims of identity theft were subject to in-depth interviews or IDIs. Open-ended questions were used in the semi-structured interviews to allow participants to freely share their experiences while ensuring vital topics of recovery and reintegration were covered. Interviews were conducted in neutral, private, and safe venues convenient to the participants, such as designated meeting rooms or other secure spaces mutually agreed upon by the participant and the researcher. Each location was arranged to ensure confidentiality, comfort, and the absence of outside interruptions.

All interviews were recorded with the participant's consent and transcribed verbatim. The transcription process ensured that all responses were accurately captured, preserving the richness of participants' narratives. After transcription, the data were then forwarded to the data analyst, who assisted in the thematic analysis and interpretation. All collected data were stored in password-protected digital folders accessible only to the researcher. Any physical documents, such as signed consent forms, were kept in a locked cabinet. Data were retained only for the duration approved by the ethics review process, after which they were securely destroyed. Participant identities were protected through the use of pseudonyms and the removal of any identifying details from transcripts and reports.

According to Braun and Clarke (2006), thematic analysis is a technique for finding, investigating, and summarizing patterns (themes) in data. It frequently interprets different facets of the study issue and, at the very least, minimally organizes and richly defines a data set. The data were analyzed using a thematic analysis approach, which involved systematically coding and classifying the responses.

Regarding ethical considerations, the researcher observed that the study met all ethical standards required by the UMERC, including following research protocols, guidelines, and standards, particularly in collecting and managing data and in the care of study participants. The researcher was mindful of the sensitive aspects of the study, including the Informed Consent Process, Voluntary Participation, Privacy, and the Confidentiality of the respondents. In the Informed Consent Process, the interview was free of technical terms and was easily understandable to the study's respondents. In

addition, all study participants were given the option to participate without coercion or penalty. Furthermore, the informants' personal information required for the study was kept private and treated with the utmost confidentiality.

The research did not present any discernible risks to the participants, whether psychological or socio-economic. The primary ethical consideration involved ensuring the privacy and well-being of the participants. Since the research primarily relied on qualitative methods, such as in-depth interviews, the risk of harm to participants was minimal. However, the researcher needed to be mindful of the subject matter's sensitivity and to employ ethical practices. Overall, with proper ethical safeguards and thoughtful content handling, the risk level in conducting this manuscript is relatively low. Finally, after complying with the UMERC requirements, the researcher received the certificate of approval with protocol number UMERC-2025-305 on August 16, 2025.

4. Results and Discussion

4.1 Lived Experiences of Identity Theft Victims

This portion delves into the lived experiences of seven (7) individuals who became victims of identity theft in Davao City. They shared their stories through in-depth interviews and focus group discussions, providing a clear window into the sudden disruptions, emotional turmoil, and practical challenges caused by the unauthorized use of their personal and work-related accounts. These narratives revealed diverse yet interconnected experiences, from the initial shock of losing access to compromised Facebook and email accounts to the psychological distress characterized by fear, anxiety, trauma, and persistent digital distrust.

Table 2: Lived experiences of individuals who have fallen victim to identity theft

Essential Theme	**Core Ideas**
Compromised Accounts	- Suffered shock due to sudden loss of access and unauthorized use of personal and work accounts [Trojan 1,2,3] - Discovered intrusion and manipulation of personal email settings, resulting in loss of control and security. [Trojan 3, 5]
Digital Distrust	- Experienced loss of confidence in online selling and social media [Trojan 3, 4] - Developed fear and distrust toward social media use [Trojan 2,6]
Emotional and Psychological Distress	- Experienced trauma, paranoia, and anxiety [Trojan 2,3,5,6,7] - Felt panic, weakness, and emotional distress. [Trojan 4,6] - Felt anger upon discovering unauthorized access to work email. [Trojan 1] - Endured mental overload and inability to concentrate [Trojan 1] - Experienced discouragement, stress, and emotional exhaustion [Trojan 4]
Occupational Disruption	- Encountered decreased productivity due to work disruptions caused by account intrusion. [Trojan 1] - Faced significant work disruptions, including loss of access to essential reports, missed deadlines, and temporary payroll inaccessibility [Trojan 3, 5]
Financial Loss	- Sustained significant income loss and customer base depletion. [Trojan 4] - Incurred additional financial burdens through transportation costs and time investment [Trojan 1]

Damaged Reputation	- Encountered client dissatisfaction after contacts received spam from the compromised account. [Trojan 3] - Suffered damaged business reputation and customer mistrust [Trojan 4]

Table 2 presents six major themes emerging from victim testimonies, representing the multidimensional impact of cybercrime victimization. These themes: Compromised Accounts, Digital Distrust, Psychological Distress, Occupational Disruption, Financial Loss, and Damaged Reputation collectively illustrate how a single incident can ripple across multiple areas of a victim's life, thus creating interconnected layers of harm that extend beyond the initial breach of security.

4.1.1 Compromised Accounts

This theme captures the initial victimization experience, characterized by sudden disruption and the violation of digital autonomy. Participants experienced immediate shock and a loss of control when they discovered unauthorized access to their personal and work accounts. Moreover, stealing information can be used to commit multiple criminal acts, such as financial fraud, unauthorized access to an account, impersonation, and even opening new accounts in the victim's name.

Huseynov (2025) argued that identity theft is a criminal act in which someone wrongfully obtains and uses another person's personal information without the individual's consent, typically for fraudulent purposes. Additionally, Swanson (2008) further supports this by stating that although identity theft is not a new crime, it has become much simpler for identity thieves to obtain, exploit, and misuse a person's personal information for fraudulent purposes due to the quick development of information technology, especially the widespread use of digital platforms, online transactions, and interconnected databases.

4.1.2 Digital Distrust

Beyond the immediate breach, victims often develop a persistent caution toward online platforms. Identity theft undermines confidence in digital environments, making users hesitant to engage in activities they previously relied on for work, communication, or social interaction.

This theme is supported by Chauhan (2023), who states that understanding and cultivating digital trust (DT) is essential for maximizing the potential of digital technologies and for upholding positive relationships with them as technology becomes increasingly integrated into our lives and businesses. Moreover, this aligns with the study by Pietrzak and Takala (2021). In recent years, digital technologies like social networks, cellphones, blockchains, and big data have become an essential part of our lives. Even in vital areas like health, finance, and education, they have a big influence on our day-to-day existence. Trust is crucial for reducing anxiety and encouraging participation, as there is greater uncertainty and perceived risk in online environments than in traditional ones.

4.1.3 Emotional and Psychological Distress

Identity theft significantly affected participants' emotional well-being, leading to trauma, anxiety, and sustained psychological strain. The result of this theme aligned with the study of Sharp *et al.* (2003), which found that the majority of participants reported an increase in maladaptive psychological and somatic symptoms following victimization. Moreover, identity theft victims do experience increased psychological and physical distress, and distress persists over time for those whose cases are unresolved and resolved.

These narratives establish that identity theft is not merely a technical or financial issue but a profound psychological stressor that can disrupt daily functioning, concentration, and emotional stability. Moreover, in the study examined by Li *et al.* (2019), they discovered that emotional and psychological distress has a positive influence on behavioral responses and that perceived victimization severity, which is based on the amount of money lost, the degree of personal information misuse, and the time spent resolving the issue, has a positive impact on perceived distress particularly due to the case of identity theft.

4.1.4 Occupational Disruption

Identity theft also disrupted participants' professional lives, affecting productivity, deadlines, and administrative responsibilities. Furthermore, being a victim of identity theft not only takes effect in the emotional and psychological aspects of the victim, but it also has an appalling effect on the victim's employment performance.

This theme is being supported by the Identity Theft Resource Center (ITRC) in 2024, which suggests that combining the effects on an organization with those on an individual employee due to an identity compromise can be a recipe for disaster, such as a drop in productivity or an increase in workplace apathy. These narratives reveal that identity theft can extend beyond personal inconvenience. It interferes with professional performance and, in some cases, potentially impacts career evaluation and advancement. The disruption underscores the interconnection between digital security and occupational stability, demonstrating that breaches have far-reaching effects beyond the technological realm. In addition, the study by Li *et al.* (2019) emphasizes that critical identity theft incidents affected victims' behavioral responses, potentially disrupting workplace performance.

4.1.5 Financial Loss

For many victims, identity theft carries significant financial consequences, especially for those reliant on online transactions or self-employment. The findings show that financial losses borne personally by victims are strongly linked to heightened physical and emotional distress, as well as negative behavioral health outcomes, particularly when these losses are examined in more detailed terms.

These experiences highlight that financial losses from identity theft are twofold: lost revenue and the hidden costs of mitigating the breach. The findings suggest that for many victims, financial strain intensifies the stress and anxiety associated with identity

theft, which creates a cycle of economic and psychological hardship. Traditionally, identity theft has been seen as a means for obtaining access to a victim's financial information for monetary gain by a perpetrator; aside from this, the expense and loss of financial freedom during their journey of identity theft have actually impacted their perspective.

Moreover, the longer it takes to resolve an identity theft incident, the greater the distress across all indicators. For self-employed individuals, identity theft can be especially damaging, as it may cause them to lose customers who begin to doubt the credibility or security of their services, ultimately leading to significant disruptions in their business operations and reductions in income (Maher & Hayes, 2024). The loss of income, coupled with expenses incurred to address the incident, creates substantial economic strain (Hummer & Rebovich, 2023).

4.1.6 Damaged Reputation

Ultimately, identity theft can undermine social and professional trust, affecting relationships and credibility. Such exposure may affect how others perceive them and increase their vulnerability to financial losses, fraud, or other forms of exploitation.

According to the study by Cross and Holt (2025), when sensitive information is compromised in a data breach, there is a clear risk of harm to individuals' personal reputations and financial security. These experiences highlight that the impact of identity theft extends beyond individual loss, affecting how others perceive victims and potentially damaging professional or social relationships. Reputational harm, therefore, represents an enduring consequence that can increase the burden of identity theft. Victims often face reputational damage when their compromised accounts are used to send spam or messages that misrepresent them.

This study is supported by Jordan *et al.* (2018), who state that reputational damage most often occurs when personal data is misused for impersonation, thereby harming the victim's reputation. Reputational damage occurs when an identity thief uses a victim's information and can result in a damaged reputation, lost career opportunities, or even innocent accusations of a crime committed by the identity thief.

4.2 Coping Mechanisms Employed by Victims of Identity Theft

Victims of identity theft encountered various coping mechanisms during their reintegration. As shown in Table 3, the coping techniques employed by the victims of identity theft for them to navigate the aftermath of the crime are the following:

1) Collective Action,
2) Emotional and Social Support,
3) Technical Support,
4) Spiritual and Professional Guidance, and
5) Digital Recovery.

Table 3: Coping mechanisms employed by victims of identity theft

Essential Themes	**Core Ideas**
Collective Action	- Sought assistance from friends to report the compromised account. [Trojan 1,2,6] - Followed advice from family and online communities to report the incident to authorities. [Trojan 1, 2]
Emotional and Social Support	- Received practical and emotional support from family and friends. [Trojan 1] - Felt motivated and reassured through continuous encouragement. [Trojan 2] - Experienced comfort and reduced worry due to family support. [Trojan 6] - Received ongoing check-ins and assistance from family and coworkers. [Trojan 5]
Technical Support	- Received technical assistance from a family member. [Trojan 3] - Received coordinated support from workmates. [Trojan 5] - Received technical assistance from professionals [Trojan 7]
Spiritual and Professional Guidance	- Used prayer and relaxation activities to manage stress. [Trojan 1] - Took a break from Facebook and engaged in spiritual reading to stay calm. [Trojan 6] - Sought spiritual guidance from a priest to ease the mind. [Trojan 3] - Received professional counseling to reduce anxiety and gain reassurance. [Trojan 6]
Digital Recovery	- Created a new account and reconnected with contacts. [Trojan 2] - Made a new page and informed customers about the hacked account. [Trojan 3]

4.2.1 Collection Action

Many victims of identity theft have experienced critical journeys where they tend to lose themselves in the middle of their recovery, due to the trauma.

This theme is supported by De Kimpe in 2020, who states that some coping strategies implemented by these victims focus on directly solving the problem, while others involve ways of coping that help a person manage the emotional or psychological stress caused by the incident. The study of Salam *et al.* in 2022 examines how online users cope with the risk of identity theft and highlights the importance of taking personal responsibility and acting promptly. It also stresses that identity theft is not just an individual problem but a societal issue that can lead to significant economic losses.

4.2.2 Emotional and Social Support

In contrast, sadness and feelings of being unsafe were reported less often. The findings also indicated that victims most commonly sought professional support through counseling, as well as emotional comfort from family members and friends.

Betz-Hamilton Axton (2022) reinforced this theme by showing that victims most frequently experienced anger or a sense of violation, followed by feelings of worry, vulnerability, and distrust toward others. Moreover, in the study of McNeely (2015), he supported that individuals with higher levels of social support are generally at a lower risk of victimization, as strong networks of family, friends, and community members can provide emotional reassurance, practical assistance, and protective resources that reduce vulnerability to criminal targeting and its adverse consequences.

4.2.3 Technical Support

In the provided theme, the victims were also provided with the technical support they needed after reporting their concerns.

In the study documented by Maher *et al.* (2024), these researchers stated that victims who reported their cases and accessed assistance from organizations such as the Identity Theft Resource Center were provided with a range of structured support measures aimed at restoring their identities and reducing the adverse impacts of victimization, reflecting the availability of professional technical assistance following the offense. Furthermore, the study by Saan *et al.* (2022) states that, aside from the comfort they receive from the trauma they have experienced, help from a family member or an organization can provide strong safety and security to victims.

4.2.4 Spiritual and Professional Guidance

Becoming a victim of identity theft could give you trauma and leave a scar; however, in the study of Satchell *et al.* in 2024, they stated in their research how holding back traumatic experiences might give them a hard time moving on and foreseeing positive results. Additionally, in the same research, their findings support the idea that spiritual or faith-based guidance plays a role in how victims *feel safe, supported, and resilient* after victimization.

This theme was extensively supported by the research of Vveinhardt and Deikus (2023), which emphasized that spiritual guidance from faith leaders, mentors, or individuals with a strong, resilient belief system can play a significant role in helping victims cope with the aftermath of traumatic experiences. Their study highlighted that such spiritual support not only facilitates emotional healing but also contributes to the restoration of psychological safety, helping victims regain a sense of stability, resilience, and personal empowerment following victimization.

4.2.5 Digital Recovery

In a recovery process, it is essential to look at the bright side despite the struggle and traumatic experiences as an aftermath of becoming a victim, especially with identity theft.

Gies and Piquero's 2020 study emphasized how tailored support from professional organizations can guide victims through the complex process of restoring their identities, including navigating digital recovery procedures, communicating with the bureaus, and even resolving fraudulent accounts. Moreover, through its analysis of effectiveness, particularly in these interventions, the study highlights the critical role that both structured and professional guidance and coordinated services play in helping victims regain control over their personal and financial information, reduce ongoing stress, and prevent further victimization.

To support this theme, Li *et al.* (2019) examined how victims of identity theft frequently respond to violations of their digital identities by altering their online behavior and implementing a variety of proactive digital strategies to cope with the incident and regain control over their personal information. These adaptive behaviors can include creating new accounts, updating and strengthening security settings, notifying friends or

customers about compromised accounts, and carefully monitoring digital platforms to prevent further misuse. By taking these steps, victims not only work to restore their online presence but also reduce the risk of repeat victimization and rebuild a sense of safety and confidence in their digital interactions.

The digital recovery, on the other hand, is considered a highlight of how individuals actively navigate both technical and behavioral measures to recover from the disruption caused by identity theft.

4.3 Insights into the Lives of Victims of Identity Theft

Victims of identity theft experienced trauma and gained life-changing insights. This table presents insights from victims of identity theft based on their personal experiences with online fraud and account compromise. Through reflecting on what they learned from these incidents, the victims identified practical lessons that they believe are valuable for protecting others in the community from similar victimization.

Table 4: Insights into the lives of victims of identity theft

Essential Themes	**Core Ideas**
Strengthen Account Protection	- Avoid sharing personal information on social media [Trojan 1,2,7] - Implement security measures such as two-factor authentication, regularly changing passwords, and unique passwords for each account.
Exercise Link Caution	- Avoid clicking links to prevent hacking. [Trojan 1] - Check the website security and avoid clicking on unclear links. [Trojan 3] - Exercise caution with Messenger links. [Trojan 6]
Verify Online Contacts	- Monitor followers and avoid links from potentially fake accounts to prevent compromise. [Trojan 7] - Be cautious about trusting people you meet on social media. [Trojan 2]
Maintain Security Vigilance	- Monitor login alerts regularly to detect unauthorized access. [Trojan 3] - Exercise caution with suspicious messages and report issues promptly. [Trojan 4] - Respond immediately to warning messages to prevent further problems. [Trojan 5] - Remain alert to all notifications to maintain account security. [Trojan 4]

4.3.1 Strengthen Account Protection

Strengthening account protection is a critical strategy to prevent identity theft and limit unauthorized access to personal information. Their empirical analysis of real-world online platforms showed that contextual indicators, particularly changes in IP address, device attributes, and login behavior, are central to identifying potential account compromise. By requiring stronger authentication only under high-risk conditions, Risk-Based Authentication effectively balances security and usability, reducing opportunities for credential misuse while minimizing user burden. These findings underscore the importance of adaptive authentication mechanisms as a proactive account protection measure that can significantly mitigate identity theft risks in digital environments.

Wiefling *et al.* (2019) demonstrated that Risk-Based Authentication enhances account security by dynamically evaluating the risk level of each login attempt and activating additional verification measures when suspicious activity is detected.

Moreover, another study by Ismailov *et al.* (2020) examined vulnerabilities in existing research on identity deception detection within online social networks, emphasizing how these weaknesses undermine effective account protection. The authors noted that identity deception, including fake profiles and impersonation, poses persistent threats to user security and facilitates identity theft in digital platforms. Their analysis revealed that many detection models rely on limited or unrealistic datasets, exhibit data-selection bias, and prioritize precision over recall, thereby failing to identify a substantial number of deceptive accounts. Weak social media security leaves you vulnerable to identity theft.

4.3.2 Exercise Link Caution

Randomly clicking on links provided in online platforms could gravely lead to identity theft victimization.

In the study of Ghalechyan *et al.* (2024), the research supported the theme, which states that they conducted an empirical study on the use of neural network models to distinguish between phishing and legitimate URLs, demonstrating the potential for machine learning to enhance the detection of malicious links that often serve as entry points for identity theft and account compromise. Maintaining vigilance when interacting with online communications, such as scrutinizing links, emails, and requests for personal information, is critical to reducing the risk of victimization from identity theft.

This notion was also supported by the study by Kayomb *et al.* (2025), which examined the reality at the South African University of Technology and found that many students, faculty, and staff lacked sufficient awareness to recognize phishing attacks, making them vulnerable to identity theft and account compromise. Moreover, by improving users' ability to critically evaluate links and detect deceptive communications, the framework directly reinforces the practice of link caution, which is essential for preventing unauthorized access, safeguarding personal information, and mitigating the risk of digital identity theft.

4.3.3 Verify Online Contacts

Online impersonation is rampant on digital platforms, as anyone can create a fake profile to contact their potential victim. A hacker can send messages to their victims freely, allowing the victims to click the link and get their information as easily as possible. Moreover, users are overwhelmed by the number of digital applications they use and by using them over time without checking their profiles. To commit malicious acts and online social crimes, scammers and adversaries create numerous false profiles.

This notion was supported by Meligy *et al.* (2017), who found that identifying users in Online Social Networks (OSNs) is an unresolved security and privacy issue. In the study of Sil and Bhattacharya (2025), it is stated that profile cloning and fake engagement techniques, which entail the creation and use of phony or automated accounts to manipulate popularity metrics, trick real users, and skew public perception, are among the most urgent security issues. These actions not only seriously jeopardize

personal privacy but also erode confidence in online interactions, distort advertising tactics, and jeopardize the platform's overall integrity.

4.3.4 Maintain Security Vigilance

It is important to be vigilant and verify suspicious profiles to eliminate the risk of identity theft. This shift exposes web applications to heightened vulnerabilities due to their accessibility, making them prime targets for cyberattacks. Innovations in data transmission pathways, security protocols, software enhancements, and related frameworks are continuously developed to safeguard sensitive information. However, technological solutions alone are insufficient.

Continuous vigilance by users and administrators, including monitoring login and logout activities, scrutinizing suspicious messages and links, and promptly responding to anomalies, is essential to prevent unauthorized access and protect digital assets. Maintaining this dual approach, with robust technical safeguards combined with proactive human vigilance, forms the cornerstone of effective cybersecurity and identity protection in the digital age.

This theme was supported by Madinaxon in 2025, and he states that as internet technologies evolve, critical business functions and services, including banking systems, e-commerce platforms, corporate websites, news outlets, entertainment services, trading platforms, blogs, and government portals, are increasingly conducted online. According to Cassim (2015), identity theft is recognized as one of the fastest-growing white-collar crimes worldwide. Its consequences are far-reaching, affecting victims' financial and emotional well-being, imposing costs on institutions, and challenging law enforcement and governments globally. He further emphasizes and supports the notion that organizations should implement strong safeguards for personal information.

At the same time, individuals remain vigilant, informed about their rights, and proactive in protecting their data both offline and online, maintaining continuous awareness, monitoring account activity, and adapting security practices to counter evolving threats.

5. Recommendation

5.1 Implication of Practice

First, financial institutions, law enforcement, and support organizations must recognize the psychological, emotional, and social impacts of identity theft. Providing immediate, empathetic, and trauma-informed assistance helps victims regain control and a sense of security.

Second, ongoing support is essential. Access to credit monitoring, legal aid, counseling, and education about personal data protection helps victims recover financially and reduces the risk of future victimization. Encouraging victims to take proactive steps, such as updating accounts, reporting fraud, and adopting digital safety practices, fosters empowerment and restores confidence.

Third, collaboration among financial institutions, law enforcement, government agencies, and victim support services is critical. Coordinated responses that address both practical and emotional needs ensure effective support. Combining legal, financial, and psychological assistance increases the chances of meaningful recovery.

Finally, public awareness campaigns and education are necessary to reduce stigma and victim-blaming. Promoting understanding that identity theft can happen to anyone encourages community support and helps victims rebuild trust in social and financial systems.

5.2 Implications for Future Research

Future studies could examine how socio-economic and cultural factors influence victims' experiences and recovery. Comparative research across different groups would provide insight into vulnerabilities and resilience strategies.

Longitudinal research tracking victims over time could reveal the long-term effects on psychological well-being, financial stability, and social relationships. Understanding these patterns would inform more effective prevention and intervention programs.

Research on technology's role in both victimization and recovery, such as fraud detection tools, online support groups, and cybersecurity education, could guide practical solutions.

Finally, exploring the perspectives of law enforcement, financial institutions, and victim advocates could highlight systemic barriers and effective strategies. Participatory research with these stakeholders may generate contextually relevant policies that enhance victim support.

6. Conclusion

Exploring the experiences of identity theft victims has been both enlightening and humbling. This study highlights the emotional, financial, and social challenges that victims face as they navigate recovery. Participants demonstrated resilience, determination, and adaptability despite feelings of violation, fear, and helplessness. Their stories show how victims rebuild trust, regain financial stability, and protect personal information.

The findings emphasize the importance of comprehensive support systems combining emotional, legal, and financial assistance. Recovery is facilitated by strong networks of family, friends, and professional support, along with accessible resources that empower victims to take proactive steps. This study also underscores the role of society, institutions, and policymakers in supporting victims. Stronger legal protections, financial safeguards, and public education are essential in reducing the impact of identity theft and associated stigma.

In conclusion, while identity theft poses significant challenges, victims' experiences show human resilience and adaptability. With coordinated support, informed policies, and a compassionate response, victims can recover, regain confidence,

and continue to thrive. This research calls for victim-centered approaches, enhanced prevention, and a society where individuals feel safe protecting their identities.

Acknowledgement

This study was made possible thanks to the priceless guidance and support of many individuals. Though they may not be mentioned by name, their contributions are sincerely and deeply appreciated. Above all, the researcher offers heartfelt gratitude to the Divine Creator, whose boundless blessings—the gift of life, wisdom, health, and the unwavering love of family and friends—have been the bedrock of resilience and inspiration throughout this academic journey.

Dr. Rowela Cartin-Pecson, the researcher's mentor, for her guidance and patience, as well as her invaluable expertise. Her insightful feedback and constructive comments contributed to the success and the quality of this study. The examination panel, led by Dr. Nestor C. Nabe, and comprising members Dr. William A. Revisa, Dr. Carmelita B. Chavez, and Dr. Joel B. Tan, for their feedback, supportive criticism, revision, and suggestions to better this study. Dr. John Harry Caballo, the researcher's data analyst, grammarian, and editor, for his commitment and professional assistance. His knowledge was essential to guaranteeing the quality and correctness of the data findings. His advice made this study possible.

I thank everyone in my family, friends who assisted me in pursuing and fulfilling my dreams by inspiring me through their patience, kindheartedness and constant love.

Conflict of Interest Statement

The authors declare no conflicts of interest.

About the Authors

Dianne Chlaire V. Duron, RCrim, is an accomplished educator and researcher within the College of Criminal Justice Education at the University of Mindanao, where she serves as an Instructor and Assistant Laboratory Custodian. Since entering the academe in 2022, she has consistently expanded her expertise in criminology and forensic science through high-level training, workshops, and professional seminars. Currently a candidate for the Master of Science in Criminal Justice at the University of Mindanao

Professional Schools, the researcher is dedicated to advancing the field through rigorous inquiry. Her scholarly work is strategically focused on law enforcement optimization, security protocols, and the evolution of the criminal justice system.

Rowela Catin-Pecson (PhD) is a professor and quality assurance expert at the College of Criminal Justice Education, University of Mindanao, and holds a Doctor of Philosophy in Criminal Justice with a specialization in Criminology from the Professional Schools, University of Mindanao, Philippines. Currently, through her active membership in the Philippine Society of Criminologist and Criminal Justice (PSCCJP), she has been actively participating in seminar training, as the facilitator, in the United States Agency for International Development (USAID) "Seminars and Training for Environmental Crime" in many parts of the country and as, resource speaker and facilitator, United States Department of Justice Office of Prosecutorial Development and Trainings (OPDAT) "Cybercrime Training of Trainers."

References

Ahmed, S. R. (2020). *Preventing identity crime: identity theft and identity fraud: an identity crime model and legislative analysis with recommendations for preventing identity crime.* Brill. Retrieved from https://brill.com/display/title/54591?language=en

Balistoy, H., Toledo, V., & Dullacin, D. (2024). *The Prevalence of Identity Theft in Davao City: Basis for an Intervention Scheme*. University of Mindanao.

Betz-Hamilton Axton. (2022). A Comparison of the Financial, Emotional, and Physical Consequences of Identity Theft Victimization Among Familial and Non-Familial Victims. *Journal of Financial Counseling and Planning, 33*(2), 217–227. https://doi.org/10.1891/JFCP-2021-0014

Cassim, F. (2015). Protecting personal information in the era of identity theft: just how safe is our personal information from identity thieves?. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad, 18*(2), 68–110. https://doi.org/10.4314/pelj.v18i2.02

Chauhan, D. (2023). Digital trust is core to our relationship with technology. *Network Security, 2023*(10) Retrieved from https://www.magonlinelibrary.com/doi/abs/10.12968/S1353-4858%2823%2970047-0

Cohen, L. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. Retrieved from https://faculty.washington.edu/matsueda/courses/587/readings/Cohen%20and%20Felson%201979%20Routine%20Activities.pdf

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage Publications. Retrieved from uk.sagepub.com/en-gb/eur/qualitative-inquiry-and-research-design/book266033

Cross, C., & Holt, T. J. (2025). Beyond fraud and identity theft: assessing the impact of data breaches on individual victims. https://www.tandfonline.com/doi/full/10.1080/0735648X.2025.2535007?utm_source=chatgpt.com#abstract

De Kimpe, L. (2020). The Human Face of CyberCrime. Identifying targets, victims, and their coping mechanisms. Retrieved from https://biblio.ugent.be/publication/8670387

DeLiema, M., Burnes, D., & Langton, L. (2021). The financial and psychological impact of identity theft among older adults. *Innovation in Aging, 5*(4). https://doi.org/10.1093/geroni/igab043

Dentzel, Z. (2017). How the Internet has changed everyday life. OpenMind. Retrieved from https://www.bbvaopenmind.com/en/article/internet-changedeverydaylife/?fullscreen=true

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

Ghalechyan, H., Israyelyan, E., Arakelyan, A., Hovhannisyan, G., & Davtyan, A. (2024). Phishing URL detection with neural networks: an empirical study. *Scientific Reports, 14*. Retrieved from https://www.nature.com/articles/s41598-024-74725-6?utm_source=chatgpt.com

Gies, S. & Piquero, N. (2020). Recover Me if You Can: Assessing Service to Victims of Identity Theft. Retrieved from https://nij.ojp.gov/library/publications/recover-me-if-you-can-assessing-services-victims-identity-theft

Harrell, E. & Thompson, A. (2023). Victims of Identity Theft, 2021. Retrieved from https://bjs.ojp.gov/library/publications/victims-identity-theft-2021

Hedayati, A. (2012). An analysis of identity theft: Motives, related frauds, techniques, and prevention. *Journal of Law and Conflict Resolution, 4*(1), 1–12. Retrieved from https://academicjournals.org/article/article1379859409_Hedayati.pdf

Hummer, D. & Rebovich, D. J. (2023). Chapter 2: Identity theft and financial loss. (p. 38–53). Retrieved from https://www.elgaronline.com/edcollchap/book/9781800886643/book-part-9781800886643-10.xml

Huseynov, E. (2025). Identity Theft. In Computer and Information Security Handbook (pp. 993–1006). Morgan Kaufmann. Retrieved from https://www.sciencedirect.com/science/chapter/edited-volume/abs/pii/B9780443132230000606

Identity Theft Resource Center (2024). The Impacts of Identity Theft on Employees and Their Workplace. Retrieved from https://www.idtheftcenter.org/wp-content/uploads/2020/08/Identity-Theft-in-the-Workplace-Aura-ITRC-Report-081420-WEB-ADA.pdf?utm_source=chatgpt.com

Ismailov, M., Tsikerdekis, M., & Zeadally, S. (2020). Vulnerabilities to Online Social Network Identity Deception Detection Research and Recommendations for Mitigation. *Future Internet, 12*(9), 148. https://doi.org/10.3390/fi12090148

Kayomb, J. M., Francke, E. R., & Ncubukezi, T. (2025). A phishing attack awareness framework for a South African University of Technology. *South African Journal of Information Management, 27*(1), a1949. (https://sajim.co.za/index.php/sajim/article/view/1949)

Kayser, C. S., Back, S., & Toro-Alvarez, M. M. (2024). Identity Theft: The Importance of Prosecuting on Behalf of Victims. *Laws, 13*(6), 68. https://www.mdpi.com/2075-471X/13/6/68

Li, Y., Yazdanmehr, A., Wang, J., & Rao, H. R. (2019). Responding to identity theft: A victimization perspective. *Decision Support Systems, 121*, 13–24. https://www.sciencedirect.com/science/article/pii/S0167923619300612

LoPucki, L. (2001). Human Identification Theory and the Identity Theft Problem. Retrieved from https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=2137&context=facultypub

Madinaxon, A. B. (2025). Identification and Prevention of Identity Theft. *International scientific journal Management, Marketing and Finance, 1*(5), 36–57. Retrieved from https://jmmf.uz/view?id=111

Maher, C. A., Corsello, R. M., Engle, T. A., Kuhlman, J. D., & Nedelec, Joseph L. (2024). *Correlates of victim services for fraud and identity theft among victim service providers,* Journal of Criminal Justice, vol. 95(C). Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0047235224001673

Maher, C. A., & Hayes, B. E. (2024). Nonfinancial Consequences of Identity Theft Revisited: Examining the Association of Out-of-Pocket Losses with Physical or Emotional Distress and Behavioral Health. *Criminal Justice and Behavior, 51*(3), 459–481. https://doi.org/10.1177/00938548231223166

Maillet, J. M. (2023, August 4). Identity Theft: Understanding the Silent Crime That Can Ruin Lives. Jarrett Maillet J.D., PC. Retrieved from https://www.mailletcriminallaw.com/identity-theft-understanding-the-silentcrime-that-can-ruin-lives/

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice, 31*(1), 30–52. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/1043986214552607

Meligy, A. M., Ibrahim, H. M., & Torky, M. F. (2017). Identity verification mechanism for detecting fake profiles in online social networks. *Int. J. Comput. Netw. Inf. Secur (IJCNIS), 9*(1), 31-39. Retrieved from. Retrieved from https://www.researchgate.net/profile/Mohamed-Torky6/publication/312137248_Identity_Verification_Mechanism_for_Detecting_Fake_Profiles_in_Online_Social_Networks/links/5bd8f04da6fdcc3a8db2c5be/Identity-Verification-Mechanism-for-Detecting-Fake-Profiles-in-Online-Social-Networks.pdf

Neira, R. E. (2016). Identity theft: Inside the mind of a cybercriminal (Master's thesis, Utica College). Retrieved from

https://www.proquest.com/openview/912fc0d5c5c4fd6424c93f40e1b5c70c/1pq-origsite=gscholar&cbl=18750

Pietrzak, P., & Takala, J. (2021). Digital trust–a systematic literature review. Retrieved from https://osuva.uwasa.fi/items/51f0d6e0-8c7e-4703-a1f3-5e1a363c3519

PNP Anti-Cybercrime Group Manila (2024). Cybercrime Cases Fall by 40.79% in the Final Week of March 2024. Retrieved from https://acg.pnp.gov.ph/cybercrime-cases-fall-by40-79-in-the-final-week-of-march-2024/

Qutoshi, S. (2018). Phenomenology: A Philosophy and Method of Inquiry. *Journal of Education and Educational Development* *5*(1) Retrieved from https://files.eric.ed.gov/fulltext/EJ1180603.pdf

Roser, M. (2023). Technology over the long run: zoom out to see how dramatically the world can change within a lifetime. Retrieved from https://ourworldindata.org/technologylong-run

Saan, M., van Wesel, F., Leferink, S., Hox, J., Boeije, H., & van der Velden, P. (2022). Social network responses to victims of potentially traumatic events: A systematic review using qualitative evidence synthesis. *PloS one, 17*(11). https://doi.org/10.1371/journal.pone.0276476

Salam, A. F., Dai, H., & Wang, L. (2022). Online Users' Identity Theft and Coping Strategies, Attribution and Sense of Urgency: A Non-Linear Quadratic Effect Assessment. *Information Systems Frontiers, 24*(6), 1929-1948. https://doi.org/10.1007/s10796-021-10194-w

Satchell, J., Dalrymple, N., Leavey, G., & Serfaty, M. (2024). "If we don't forgive, it's like holding on to them": A qualitative study of religious and spiritual coping on psychological recovery in older crime victims. Psychological trauma: theory, research, practice and policy, 16(4), 643–652. https://doi.org/10.1037/tra0001420

Sharp, T., Shreve-Neiger, A., Fremouw, W., Kane, J., & Hutton, S. (2003). Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Sciences, 49*(1). https://store.astm.org/jfs2003178.html

Swanson, A. (2008). Identity Theft, Line One. Collector, 73(12), 18-22,24-26. Retrieved from https://www.proquest.com/trade-journals/identity-theft-line-one/docview/223219430/se-2

Tadros, V. (2011). *The ends of harm: The moral foundations of criminal law.* OUP Oxford. Retrieved from https://global.oup.com/academic/product/the-ends-of-harm-9780199554423?cc=bg&lang=en&

Tenny, S., Brannan, J. M., & Brannan, G. D. (2017). *Qualitative study*. Retrieved from https://europepmc.org/article/NBK/nbk470395

Van der Meulen, N. (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). Retrieved May 20, 2007. Retrieved from https://research.tilburguniversity.edu/en/publications/the-challenge-of-countering-identity-theft-recent-developments-in/

Vveinhardt, J. & Deikus, M. (2023). The use of religious resources in helping victims of workplace mobbing. *Frontiers in Psychology. Vol. 14.* https://doi.org/10.3389/fpsyg.2023.1288354

Wiefling, S., Lo Iacono, L., & Durmuth, M. (2019). *Is this really you? An empirical study on risk-based authentication applied in the wild*. In Financial Cryptography and Data Security (pp. 134 to 153). Springer. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-22312-0_10