Identity Theft Victims’ Understandings of Incidents and their Reporting Decisions

by

Dylan Reynolds

A Thesis
presented to
The University of Guelph

In partial fulfilment of requirements for the degree of Doctor of Philosophy in Sociology

Guelph, Ontario, Canada
© Dylan Reynolds, May, 2022
ABSTRACT

IDENTITY THEFT VICTIMS’ UNDERSTANDINGS OF INCIDENTS AND THEIR REPORTING DECISIONS

Dylan Reynolds
University of Guelph, 2022
Advisor: Dr. Ryan Broll

Identity theft, the theft and misuse of another person’s identity information, has increased in North America over the past decade, with almost 10 percent of adults victimized annually. Although few victims pay out of pocket for identity theft incidents, other consequences can include lost time and emotional, relational, and physical tolls. Despite these costs to millions of North Americans annually, most incidents are reported to financial institutions rather than police. In Canada, no representative identity theft victim surveys have been administered since its criminalization, and little is known about the scope and nature of identity theft. Two recent studies have examined identity theft reporting in the United States, but few studies have explored victims’ experiences qualitatively. This study employs a symbolic interactionist perspective to better understand victims’ perceptions of identity theft and their reporting decisions. Drawing from interviews with 20 identity theft victims in Ontario and quantitative analysis of the United States’ 2016 National Crime Victimization Survey – Identity Theft Supplement, it finds that victims’ understandings of the incidents they faced are processes and that identity theft is conceptualized in multiple ways: including as crimes, routine inconveniences, institutional failures, and relational issues. Many participants resisted identification as a victim for various
reasons, including that they felt they experienced little harm or that they held some blame for the incident. In terms of reporting, quantitative analyses revealed that more serious incidents were reported to law enforcement and that the reporting of victims who paid out of pocket was impacted differently by other measures of seriousness compared to those who recuperated losses.

Interview participants often took the actions they saw as practical based on their understanding of the incident, while their reporting decisions were also influenced by emotional reactions and advice. Finally, participants’ reporting experiences varied significantly: while some had their needs met promptly, others had to call institutions repeatedly or were referred elsewhere. This study makes important contributions to the existing research on identity theft victimization, and future research should continue examining this understudied area since the results suggest that many victims may fall through the cracks of victim support.
ACKNOWLEDGEMENTS

Thank you to my advisor, Dr. Ryan Broll, and my advisory committee members, Dr. Andy Hathaway and Dr. David Walters, for your teachings, feedback, and support. Thank you to the participants who shared their stories and taught me so much. Thank you to my examiners, Dr. Michael Adorjan and Dr. Myrna Dawson, for your time and expertise. Finally, thank you to the countless others who have supported this project directly or indirectly along the way.
# TABLE OF CONTENTS

Abstract........................................................................................................................................... ii

Acknowledgements......................................................................................................................... iv

Table of Contents .............................................................................................................................. v

List of Tables .................................................................................................................................. xi

List of Figures ................................................................................................................................. xii

List of Appendices ........................................................................................................................... xiii

1 Introduction................................................................................................................................. 1
   1.1 Background ........................................................................................................................... 1
   1.2 Theoretical Framework ......................................................................................................... 5
   1.3 Research Questions ............................................................................................................... 7
   1.4 Methods ............................................................................................................................... 9
   1.5 Overview ............................................................................................................................. 12

2 Theoretical Framework............................................................................................................... 15
   2.1 Introduction ........................................................................................................................ 15
   2.2 Symbolic Interactionism’s Premises .................................................................................. 17
   2.3 Selves, Identities, and Roles ............................................................................................. 20
   2.4 Self-Labeling and Becoming ............................................................................................ 23
   2.5 The Symbolic Interactional Nature of Emotions ............................................................... 26
   2.6 Role-Taking Emotions ....................................................................................................... 28
   2.7 The Construction of Social Problems ............................................................................... 31
   2.8 Social Problems and Identities ......................................................................................... 35
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.9</td>
<td>Summary</td>
</tr>
<tr>
<td>3</td>
<td>Literature Review</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>3.2</td>
<td>Identity Theft Definitions, Prevalence Estimates, and Consequences</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Identity Theft and Fraud</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Prevalence</td>
</tr>
<tr>
<td>3.2.3</td>
<td>Consequences</td>
</tr>
<tr>
<td>3.3</td>
<td>Victims’ Experiences &amp; Becoming a Victim</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Experiencing Identity Theft</td>
</tr>
<tr>
<td>3.3.2</td>
<td>Becoming a Victim</td>
</tr>
<tr>
<td>3.3.3</td>
<td>Responsibility, Blame, and Stigma</td>
</tr>
<tr>
<td>3.4</td>
<td>Victim’s Reporting Decisions and Experiences</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Identity Theft Victim Reporting</td>
</tr>
<tr>
<td>3.4.2</td>
<td>Victim’s Experiences with Institutions</td>
</tr>
<tr>
<td>3.5</td>
<td>Summary</td>
</tr>
<tr>
<td>4</td>
<td>Methods</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>4.2</td>
<td>Mixed Methods Approach</td>
</tr>
<tr>
<td>4.3</td>
<td>Quantitative Methods</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Data</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Variables</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Method of Analysis</td>
</tr>
</tbody>
</table>
4.4 Qualitative Methods ................................................................................................................. 82
  4.4.1 Recruitment ......................................................................................................................... 82
  4.4.2 Surveys ................................................................................................................................. 85
  4.4.3 Interviews ............................................................................................................................. 86
  4.4.4 Coding .................................................................................................................................. 90
4.5 Summary ..................................................................................................................................... 92
5 Results 1: Victims’ Understandings of Identity Theft and Self ......................................................... 93
  5.1 Introduction .............................................................................................................................. 93
  5.2 The Events Experienced ......................................................................................................... 94
  5.3 Defining Identity Theft Incidents .............................................................................................. 95
    5.3.1 As Crime ............................................................................................................................. 96
    5.3.2 As Routine Inconveniences ............................................................................................... 100
    5.3.3 As Institutional Failures ..................................................................................................... 102
    5.3.4 As Relational Issues and Betrayals ..................................................................................... 105
    5.3.5 Intersections of Dimensions ............................................................................................... 106
  5.4 Uncertainty and Processes of Definitions ................................................................................ 107
    5.4.1 How Discovery and Messaging Informs Conceptualization ............................................. 112
    5.4.2 Comparisons to Other Cases of Identity Theft and Fraud ............................................... 114
  5.5 Victims on Selves .................................................................................................................... 116
    5.5.1 Victim Status ....................................................................................................................... 118
    5.5.2 “Technically I Was, But…”: Resistance to the Victim Label .......................................... 119
    5.5.3 Comparisons to Typical Victims of Identity Theft ............................................................. 121
5.5.4 Self-Blame and Denying a Victimization Occurred ........................................... 124
5.6 Summary ............................................................................................................. 126
6 Results 2: Victims Reporting Decisions and Experiences with Reporting .............. 129
   6.1 Introduction .................................................................................................... 129
   6.2 Quantitative Results: Reporting to Law Enforcement, Financial Institutions, and Credit Bureaus ................................................................. 130
       6.2.1 Descriptive Statistics ............................................................................. 130
       6.2.2 Reporting to Law Enforcement ............................................................... 133
       6.2.3 Reporting to Financial Institutions ....................................................... 139
       6.2.4 Reporting to Credit Bureaus ................................................................. 143
       6.2.5 Summary ............................................................................................... 148
   6.3 Qualitative Reasoning for Reporting to Institutions ...................................... 150
       6.3.1 How Framing Informs Reporting & Perception of a Reporting Hierarchy .... 150
       6.3.2 Advice and Support in the Aftermath ...................................................... 156
       6.3.3 Emotional Reactions ............................................................................. 157
   6.4 “No Harm, No Foul”: Reasons for Not Reporting to Police ......................... 160
       6.4.1 The Incident Was Resolved Another Way .............................................. 161
       6.4.2 “RCMP is like a Big Deal”: The Incident Was Not Seen as Sufficiently Serious for Police ................................................................. 162
       6.4.3 Unsure of Practicality of Reporting ........................................................ 164
       6.4.4 Not Sure What to Do & Lack of Awareness ........................................... 166
       6.4.5 Reporting Would Create Work .............................................................. 167
6.5 “It’s Like You’re Screaming into the Void”: Victims’ Reporting Experiences ........ 168

6.5.1 Satisfaction .............................................................................................................. 169

6.5.2 Transferring from Department to Department .................................................. 171

6.5.3 Hounding for Help & Unmet Timelines .............................................................. 172

6.5.4 Belief That the Process Could Have Been More Straightforward ................. 174

6.5.5 Lack of Closure .................................................................................................... 176

6.5.6 Feeling Unheard & That Employees Did Not Want to Help ......................... 177

6.6 Summary .................................................................................................................... 180

7 Discussion ...................................................................................................................... 182

7.1 Introduction .............................................................................................................. 182

7.2 How Individuals Understand Identity Theft and Themselves ......................... 183

7.2.1 The Process of Identity Theft Victimization ..................................................... 183

7.2.2 Understandings of Identity Theft .......................................................................... 184

7.2.3 Criminality and Victim Statuses .......................................................................... 187

7.3 Victims’ Reporting Decisions .................................................................................. 189

7.3.1 Similarities Between Samples ............................................................................. 190

7.3.2 Differences Between Samples ............................................................................ 192

7.3.3 Quantitative Findings ......................................................................................... 194

7.3.4 Qualitative Findings .......................................................................................... 197

7.4 The Resolution of Identity Theft ............................................................................. 199

7.5 Policy Implications .................................................................................................. 204

7.6 Directions for Future Research .............................................................................. 206
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.7</td>
<td>Summary</td>
<td>208</td>
</tr>
<tr>
<td>8</td>
<td>Conclusion</td>
<td>210</td>
</tr>
<tr>
<td>8.1</td>
<td>Summary: Reflecting on the Research Questions</td>
<td>210</td>
</tr>
<tr>
<td>8.2</td>
<td>Contributions</td>
<td>213</td>
</tr>
<tr>
<td>8.3</td>
<td>Limitations</td>
<td>217</td>
</tr>
<tr>
<td>8.4</td>
<td>Final Thoughts</td>
<td>220</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>222</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 5-1: Forms of Identity Theft Experienced by Participants................................................. 94
Table 6-1: Descriptive Statistics (n = 5,753) .................................................................................. 131
Table 6-2: Logistic regression predicting identity theft victims reporting to law enforcement (n = 5,753) .................................................................................................................. 135
Table 6-3: Logistic regression predicting identity theft victims reporting to law enforcement (n = 5,753) .................................................................................................................. 137
Table 6-4: Predicted Probabilities of Identity Theft Victims’ Reporting to Law Enforcement Based on Distress Experienced, by Out-of-Pocket Loss (n=5,753).............................................. 138
Table 6-5: Logistic regression predicting identity theft victims reporting to financial institutions (n = 5,753).................................................................................................................. 140
Table 6-6: Logistic regression predicting identity theft victims reporting to financial institutions (n = 5,753).................................................................................................................. 142
Table 6-7: Logistic regression predicting identity theft victims reporting to credit bureaus (n = 5,753).................................................................................................................. 144
Table 6-8: Logistic regression predicting identity theft victims reporting to credit bureaus (n = 5,753).................................................................................................................. 146
LIST OF FIGURES

Figure 6-1: Predicted probabilities of reporting to law enforcement based on time spent resolving incidents for those suffering out-of-pocket losses and those recuperating losses ....................... 138

Figure 6-2: Predicted probabilities of reporting to credit bureaus based on amount taken for those suffering out-of-pocket losses and those recuperating losses .......................................................... 147

Figure 6-3: Predicted probabilities of reporting to credit bureaus based on time spent resolving incidents for those suffering out-of-pocket losses and those recuperating losses ....................... 148
LIST OF APPENDICES

Appendix A: Coding for the Quantitative Variables in this Study ........................................ 240
Appendix B: NCVS – ITS Questionnaire ............................................................................... 242
Appendix C: Image of Recruitment Poster ......................................................................... 244
Appendix D: Interview Participant Survey .......................................................................... 245
Appendix E: Interview Guide .............................................................................................. 248
Appendix F: Complete Logistic Regression Tables for Tests of Interaction Effects .......... 250
1 Introduction

1.1 Background

Identity theft, or the theft and misuse of identity information, has increased in North America in the past decade (Harrell 2019; Moreau 2021). Based on victimization surveys, approximately seven to ten percent of North American adults are victim to identity theft annually (Harrell 2019; Harrell 2021; Sproule and Archer 2008), and consequences can include losses of time and money as well as emotional, physical, and relational effects (Golladay and Holtfreter 2017; Identity Theft Resource Center 2018; Randa and Reyns 2020). Nonetheless, few victimizations are reported to law enforcement, with only 13 percent of Canadians and 7 percent of Americans reporting according to the most current estimates (Harrell 2021; Sproule and Archer 2008).

Canada’s most recent representative victimization estimates stem from a 2008 survey of identity theft victims (Sproule and Archer 2008), which predates the Canadian legal code changes that criminalized identity theft (Bill S-4 2009). At that time, identity theft and fraud were estimated to have impacted 1.7 million Canadian adults in one year (Sproule and Archer 2008). Yet even with its criminalization enacting new power to law enforcement and with recent increases in police-reporting (Allen 2018; Moreau 2019; Moreau 2021), fewer than 30,000 identity theft and fraud cases were recorded by law enforcement in 2020 (Moreau 2021). Regardless of whether enforcement is practical based on jurisdictional and logistical issues faced by police,¹ this underreporting implies that law enforcement are made aware of only a small

¹ For example, Wall (2008) discussed cultural and logistical barriers to policing identity-related crimes in the UK and Cross (2020) described Australian jurisdictional issues in responding to online fraud.
proportion of incidents. When combined with the limited Canadian research on identity theft victims, this suggests that little is known about the scope and nature of identity theft in Canada.

More is known about identity theft in the United States, where the Bureau of Justice Statistics administers the National Crime Victimization Survey – Identity Theft Supplement (NCVS – ITS) every two years. The most common form of identity theft in the United States is the misuse of an existing account, including credit card, bank, or other company accounts (Harrell 2021). Identity information can be stolen and misused either online, including through phishing scams, hacks, or breaches, or offline, such as through the theft of documents (Archer et al. 2012). However, the relative prevalence of offline and online forms remains unknown, in part because only one quarter of identity theft victims know how offenders obtained their information (Harrell 2021).

Although most identity theft victims are reimbursed by credit card companies, banks, or other companies, identity theft is far from a victimless crime (Golladay and Holtfreter 2017; Randa and Reyns 2020). Twelve percent of American victims still face out-of-pocket losses from identity theft victimization (Harrell 2021), and those with lower incomes and educational attainments are more likely to lose their own money (Reynolds 2021). Even those who recuperate losses can face secondary financial consequences, including credit issues, missed work, and financial stress (Identity Theft Resource Center 2018). Moreover, recuperating losses takes time: although most victims resolve incidents in under a day, some cases take months or longer to resolve (Harrell 2021). Of course, identity theft victimization can also produce a range of emotional consequences, including fear, anxiety, and a loss of trust (Identity Theft Resource
Center 2018). Finally, physical and relational consequences can also result from victimization (Golladay and Holtfreter 2017; Identity Theft Resource Center 2018; Reyns and Randa 2020).

The underreporting of identity theft is not well understood. While most victims in the United States report to financial institutions, fewer report to police than pay out-of-pocket for their losses (Harrell 2021). Two recent American studies have examined the factors influencing reporting. Reyns and Randa (2017) studied the effects of measures of seriousness on police reporting and found that paying out-of-pocket for losses, greater amounts taken, and greater distress all increased victims’ police reporting. In contrast, Golladay (2017) investigated how sociodemographic and situational factors influence reporting to police, financial institutions, and credit bureaus, finding that the effects of predictors varied based on the different reporting options. Of the measures of seriousness Reyns and Randa (2017) identified, Golladay (2017) only tested the effect of the amount taken; the effects of all measures of seriousness on victims’ other reporting decisions thus remain unknown.

With victims reporting to a variety of actors following identity theft (Harrell 2021), the institutional arrangement that responds to incidents appears complex. While there is a dearth of qualitative studies of identity theft victims’ experiences, Australian studies have found that fraud victims are sometimes unsure of institutions’ roles or where to report fraud (Cross 2018d; Cross et al. 2016). Most American identity theft victims indicate they did not report to police because they dealt with identity theft another way, while others express that they were unsure of what to do or did not think police would help (Harrell 2019). Thus, the underreporting of identity theft to the police may relate to how victims conceptualize responsibility for incidents, and the low
reporting rates suggest that many individuals may see identity theft as an issue for private companies.

The messaging about identity theft from media and other institutions also appears somewhat unique compared to traditional crimes, as individuals are often framed as responsible for their own protection (Cole and Pontell 2006; Monahan 2009; Whitson and Haggerty 2008). For example, most media stories on identity theft cases provide numerous tips for citizens to take to avoid victimization, from purchasing a shredder to never providing financial information electronically (Cole and Pontell 2006). Moreover, North American law enforcement recommend a lengthy list of individual protective measures yet, simultaneously, depict identity theft as inevitable regardless of citizens’ preventative actions (Whitson and Haggerty 2008). In this sense, messaging often frames individuals as responsible for preventing identity theft, while neglecting the role of institutions and governments in enabling perpetrators’ access to identity information, including through insecure databases and inadequate security practices (Cole and Pontell 2006; Monahan 2009; Whitson and Haggerty 2008). Cole and Pontell argued that the overall message is that identity theft is too widespread to be prevented by police; rather, “‘the solution’ offered to the consumer is to become a less vulnerable target than one’s neighbor; in other words, let it happen to someone else” (2006:142; emphasis in original). Nonetheless, qualitative studies have yet to examine victims’ understandings of identity theft or their perceptions of responsibility for identity theft incidents.

Outside of North America, research on fraud victims, generally, suggests that a victim-blaming discourse surrounds fraud (Button and Cross 2017; Cross 2015). Victims of fraud are often constructed as gullible or greedy after falling for phishing scams, romance frauds, and
advance-fee frauds (Cross 2015), which can lead to embarrassment and cause victims to hide incidents from friends and family or to not report them formally (Burgard and Schlembach 2013; Cross 2015; Cross 2018b). Scholars have not examined whether victim-blaming discourses and self-blame surround identity theft and function as a similar barrier to help-seeking.

Finally, even if victims report to companies, financial institutions, or law enforcement, little is known about how victims’ needs are met. Internationally, fraud victims have been described as often facing a “merry-go-round” effect (Button, Lewis and Tapley 2009:33), whereby institutional actors refer them to other institutions to seek help (Button et al. 2009; Button et al. 2012; Cross 2018d). In Canada, Sproule and Archer (2008) found that many victims expressed displeasure with the institutions they contacted, yet no research has examined how institutions are meeting the needs of Canadian victims since identity theft’s criminalization. As such, little is known about whether Canadians are recuperating losses or slipping through the cracks of victim support.

1.2 Theoretical Framework

Studies examining victims’ reporting decisions largely neglect the meaning that victims derive from the crimes they report, despite these meanings informing reporting decisions. Accordingly, this study employs a symbolic interactionist perspective in seeking to better understand victims’ experiences of identity theft and their reporting decisions. Building on the work of Mead, interactionists emphasize that interactions and the meanings of social objects are central to social action (Blumer 1969). Moreover, interactionism’s principles include that individuals and phenomena are formed through interactions, that symbolization is central to human group life, that humans are active in their environment, and that social interactions can
result in emergence and change (Snow 2001). These principles, along with past interactionist contributions to social problems, selves, and emotions, provide a framework for exploring victims’ understandings and experiences of identity theft victimization.

Blumer’s three premises of symbolic interactionism are that meaning is central to action, constructed through interactions, and modified during interpretation (Blumer 1969). In short, the meaning that social objects hold for individuals relates to their prior experiences and interactions. Moreover, interactionist-based contributions have emphasized the definitional nature of social problems by studying the claims made about social problems rather than treating them as objective conditions to be solved (Blumer 1971; Spector and Kitsuse [1977] 2009). Although most of these contributions focus on primary statements about problems by claims makers or secondary claims by media (Best 2003), there is also value in understanding the meaning that social problems hold for citizens, including whether conditions “assume prominence as problems” (Sasson 1995:3). In this sense, even when social problems gain attention, they may be framed in multiple ways based on who or what is constructed as responsible for the condition (Loseke 2017). For example, framing drug use as a crime attributes responsibility to the drug user in a way that framing it as a public health issue may not. Taken together, interactionism and social problems research inform the study of victims’ understandings of the events they experience.

Interactionism has also illuminated processes through which individuals take the self as object (Mead 1934), which can result in self-defining with a range of roles, labels, group memberships, and social statuses (Rosenberg 1981). Interactionists posit that self-definitions relate to individuals’ choices of actions (ibid). For example, labeling theory concerns itself not
only with how individuals react to being labeled as deviant, but also to how embracing a deviant self-identity can influence subsequent action (Becker [1963] 1973; Lemert 1951). Changes in self-definitions can stem from external definitions, but also from changes in subgroups with which one interacts (Becker [1963] 1973) and from comparisons of the self with social depictions of groups (Link 1987; Link et al. 1989). These contributions examining changes in self-definitions provide a set of sensitizing concepts that inform understanding individuals’ acceptance and resistance to the victim label.

An interactionist approach implies that action is informed by the meaning that social objects, including the self, hold for individuals. Thus, although variations in victims’ reporting decisions are often explained through differences in crime seriousness (Xie and Baumer 2019), the meaning of events is likely to be even more central. Scholars have also noted the role of interactions (Greenberg and Beach 2004; Mason and Benson 1996) and emotions (Greenberg and Beach 2004) in informing property crime reporting decisions; both are factors to which interactionists have attended. Shott (1979) described the importance of role-taking emotions, including shame, embarrassment, and pride, that result from taking other individuals’ perspectives while viewing the self. Experiencing emotions like embarrassment can inform individuals’ choices of action and disclosure (Goffman 1963; Shott 1979). With evidence that fraud victims may be stigmatized (Cross 2015), these contributions are beneficial for understanding identity theft victims’ reporting decisions.

1.3 Research Questions

With a desire to better understand identity theft victims’ understandings, reporting decisions, and experiences, this study is guided by the following research questions:
1. a) How do those who have experienced identity theft understand the events – be it as crimes, inconvenient events, or otherwise?
b) Do those who experience identity theft victimization identify themselves as victims of crime?
2. a) Do those who have experienced identity theft formally report it? If so, to whom?
b) Why do those who have experienced identity theft choose to report or not report to specific institutions (e.g. police, credit card company, etc.)?
3. How satisfied are victims with the resolution facilitated by the institutions they approach?

Little is known about North American identity theft victims’ experiences and perceptions of victimization. However, with more incidents reported to private companies than law enforcement and with messaging that frames identity theft as inevitable while placing responsibility on individuals (see Cole and Pontell 2006), it is worthwhile to assess how victims understand the incidents they face. Moreover, from an interactionist perspective, it is expected that the way that victims understand both identity theft and the self following victimization would inform their reporting decisions. While American identity theft victims’ reporting decisions have been examined quantitatively in two studies (Golladay 2017; Reynolds and Randa 2017), these could not capture victims’ attitudes and assumptions about the incidents they faced and the institutions responsible for their resolution.

Moreover, investigating victims’ satisfaction with the resolution of identity theft is important for multiple reasons. First, it may afford a better idea of whether and which victims are being supported by Canadian institutions. Second, with many North American adults likely to face multiple identity theft victimizations in their lifetime, one’s experiences with responding institutions are expected to inform future reporting decisions.
1.4 Methods

This study draws from 20 active interviews with victims of identity theft in Southern Ontario as well as quantitative analysis of the 2016 NCVS – ITS. Specifically, this study’s second research question, regarding victim reporting decisions, draws from mixed methods while the remaining research questions are informed by analysis of interview data. While identity theft laws are similar in the United States and Canada, the analyses stem from data from different social contexts and must be interpreted as such; thus, they are intended as separate exploratory contributions to knowledge about identity theft in North America.

Quantitative analysis of the 2016 NCVS – ITS is used in conjunction with qualitative data to answer this study’s second research question in examining patterns in reporting decisions. In Canada, no representative victimization surveys of identity theft have been conducted since Sproule and Archer’s in 2008, which was administered prior to the assent of the bill criminalizing identity theft. In contrast, the NCVS – ITS is the most comprehensive representative identity theft victim survey for assessing the prevalence, characteristics, and consequences of identity theft as well as victims’ reporting decisions.

In the United States, two studies have examined reporting decisions using the 2012 NCVS – ITS. Reyns and Randa (2017) examined how measures of seriousness inform police reporting, but they did not examine the other institutions to which victims often report. In contrast, Golladay (2017) investigated reporting to law enforcement, financial institutions, and credit bureaus, but included only one measure of seriousness, the amount taken, despite Reyns and Randa (2017) finding that suffering out-of-pocket loss and distress were also significant factors in reporting. Accordingly, this study uses quantitative analysis to further explore the
relationships between measures of seriousness and reporting to law enforcement, financial institutions, and credit bureaus. Moreover, unlike past studies, this study examines the effect of time spent resolving incidents on reporting, which has been found to influence perceptions of identity theft’s seriousness (Li et al. 2019). Finally, quantitative analysis allows for the exploration of relationships between predictor variables, including whether out-of-pocket loss moderates the effects of other measures of seriousness. Thus, this study’s quantitative analysis enables the most comprehensive exploration of factors influencing identity theft victim reporting decisions to date.

In addition, active interviews were conducted with victims of identity theft to provide qualitative insight into identity theft victimization, an area which has typically been examined quantitatively. Legal terms, including identity theft, were not used in the recruiting process with the goal of inviting participants regardless of how they conceptualized their misused identity information and accounts. An active interviewing approach recognizes the interactional dynamics of interviews, allowing the interviewer to implement techniques to shift the context of the interaction and attempt to evoke responses that reveal participants’ underlying assumptions (Holstein and Gubrium 1995). Interviews began with a narrative component, where participants recounted their experience(s) with identity theft victimization. Subsequent follow-up questions and open-ended conversation then permitted further exploration of participants’ perceptions of identity theft and its responsibility in society. At times, the interviewer encouraged more detailed responses by embracing their status as someone who had not experienced identity theft or by more directly challenging participants’ answers to shift the interactional setting.
This study is thus positioned to provide the most insightful qualitative assessment of identity theft victims’ perceptions, experiences, and reporting decisions to date. The recruiting and interviewing approaches enabled participants to describe incidents which could legally be defined as identity theft in their own words, while allowing the interviewer to further attempt to gauge participants’ underlying assumptions. In this sense, these approaches are well-situated to answer this study’s first research questions about victims’ understandings of events and themselves. This enables a better understanding of whether Canadian victims view the events they face as crimes and themselves as victims, and whether and how these incidents are problematized or normalized.

While quantitative exploration of the NCVS – ITS allows for an analysis of patterns in American victims’ reporting decisions, interviews provide a richer understanding of victims’ reasoning. Moreover, qualitative analyses enable an assessment of how various interactional and social factors inform reporting decisions, including emotions, interactions with loved ones and others, and perceptions of the self, the incident, and responding institutions’ roles. In turn, this study explores the characteristics of victimizations reported to the various responding institutions as well as the reasons for participants’ decisions to contact and not contact specific institutions. This can also provide an indication of the types of victimizations that go unreported to those who could assist. Relatedly, interview data are used to answer this study’s third research question and understand participants’ experiences with reporting and satisfaction with responding institutions, including whether their needs were met. In sum, while analysis of the NCVS – ITS explores the effects of quantifiable factors on reporting decisions, interviews enable a deep assessment of how
victims understand identity theft and its responding institutions and how these understandings inform reporting decisions.

1.5 Overview

The rest of this dissertation is organized as follows. Chapter 2 presents this study’s theoretical framework. Symbolic interactionism represents an approach to the social world that focuses on joint action and symbolization. Interactionist contributions have presented sensitizing concepts related to identities, symbols, emotions, and social problems that inform this study. In Chapter 3, I situate the present study’s research questions within existing scholarship on victims of identity theft, fraud, and other crimes. Chapter 4 presents this dissertation’s methodological approach, including the method of analysis of the 2016 NCVS – ITS and the recruiting, interviewing, and analytic techniques for qualitative interviews.

Chapter 5 and 6 present the results of this dissertation. In answering this study’s first research question in Chapter 5, I argue that victims frame identity theft incidents in multiple ways, including as crimes, inevitable inconveniences, relational issues, institutional security failures, and mistakes. Moreover, victims’ understandings of identity theft incidents are processes and their definitions of events often change over time, including through internet searches and by talking to institutional actors. Chapter 5 also presents the argument that although some of those who experience identity theft accept a victim label, others resist identification as such. Victims frequently devalued the harm experienced or downplayed that a victimization occurred by attributing some fault to themselves. At times, participants who downplayed the harm they experienced did so through comparisons to stereotypical victims of identity theft who were viewed as having it worse, including the naïve and the elderly. Thus, although the
participants in this study faced a range of harm, including emotional, relational, financial, and other consequences, many downplayed that harm and some understood incidents as inevitable and non-criminal.

Chapter 6 addresses the study’s final two research questions. The chapter begins by presenting analyses of the NCVS – ITS which find that increases in measures of seriousness predicted greater likelihoods of reporting to law enforcement and credit bureaus, but that their effects on reporting to financial institutions varied. Additionally, this study found significant interaction effects between suffering out-of-pocket loss and other measures of seriousness on reporting to law enforcement and credit bureaus. These suggest that the reporting decisions of victims who suffer out-of-pocket loss are less impacted by other measures of seriousness than those who recuperate losses. Drawing from interview analysis, I also argue that victims’ reporting decisions often related to their framing of incidents; how participants understood incidents related to their views of the incidents’ practical solutions, thus informing reporting decisions. Additionally, victims’ reporting decisions were sometimes informed by their emotional reactions, including embarrassment, and by advice received from loved ones and institutional actors.

Finally, in Chapter 6, I also argue that victims of identity theft faced significantly different experiences when dealing with institutional actors, even when circumstances of the incidents appeared similar. While some participants were satisfied with institutions, including when they reimbursed charges promptly or provided notices of suspicious transactions, other participants had to call institutions repeatedly, call multiple institutions, or felt that institutions provided no closure.
Chapter 7 situates these results in the context of past research on victims of crime, including identity theft and fraud. Despite its relatively recent criminalization, law enforcement appear to play only a minor role in responding to identity theft. The differing reporting experiences of victims suggest that the current institutional arrangement responding to victims provides unequal support and leads some victims to go unassisted. This chapter closes with the presentation of policy implications and suggestions for areas of future research based on this study’s findings. Finally, Chapter 8 revisits this study’s research questions and addresses this study’s contributions and limitations.
2 Theoretical Framework

2.1 Introduction

Literature examining victims’ reporting decisions in the aftermath of crimes is limited, drawing primarily from positivist conceptions of crime, victims, and seriousness. Although theories of police reporting have moved beyond simple rational choice models to account for factors such as external advice and perceptions of police (Xie and Baumer 2019), these contributions largely neglect meaning and the individual’s role in mediating their social contexts. This study of identity theft victimization exists at the intersection of several fields, including victimology, the sociology of emotions, cyber-criminology, and social problems. Few scholars took victims as the object of study until the mid-20\textsuperscript{th} century when positivists began identifying typologies of victims (Miers 1989). Interpretivists, however, have challenged positivist conceptions of victims by posing questions such as: “who is the victim?” (Quinney 1972) and “when and with what consequences does a person understand himself or herself to have become some existential entity called a victim?” (Rock 2002:19). These are important for a common yet rapidly evolving crime like identity theft that can take many forms (Harrell 2019). Further, victimologists have long understood the many emotions that can arise from criminal victimization. In the aftermath of identity theft, victims report emotions that are similar to other crimes such as anger, frustration, and feelings of vulnerability (Golladay and Holtfreter 2017; Identity Theft Resource Center 2018) but may also face relatively unique emotions such as embarrassment and shame (see Cross 2015). These emotions may influence reporting decisions in identity theft’s aftermath.
Identity theft research also exists at the margins of cyber-criminology and victimology. The expanding use of electronic payment systems and online data storage is credited as a key driver in increasing rates of identity theft (Anderson, Durbin, and Salingger 2008). Online forms of identity theft can include hacking or phishing, while offline forms can include the theft of identity documents and dumpster diving for personal information. Identity theft is somewhat unique among so-called cybercrimes since most victims are unsure of how their information is taken and misused (Harrell 2019). Finally, social problems literature can inform the examination of the understandings that individuals hold about identity theft (see Sasson 1995). The amount of identity theft incidents that go unreported to police and the changing forms of identity theft result in uncertainty about how identity theft is understood within society. As such, it remains unclear how these events are conceived and whether they “assume prominence as problems” (ibid:3). Finally, victims’ actions in the aftermath of identity theft are likely informed by whether their experiences align with their prior conceptions of identity theft and its victims.

This study is situated within a symbolic interactionist framework, drawing from past contributions to areas such as identity formation, self-labeling, emotions, and social problems. Most explicitly addressed in Maines’s (2001) discussions of “interactionist promoters,” “utilizers,” and “unaware interactionists” (pp. 15-6), symbolic interactionism has informed much contemporary sociological thought, even when it goes unacknowledged (Atkinson 2015; Fine 1993; Maines 2003; Ulmer 2003). Since much remains unknown about victims’ experiences of

---

2 Dumpster diving is the act of searching for valuable items in dumpsters or other garbage and recycling receptacles.
their victimization, the concepts described below are intended to be viewed as sensitizing concepts from which to begin analysis rather than as definitive phenomena (Blumer 1954).³

This chapter begins by discussing central premises outlined by symbolic interactionists. Following this, interactionist contributions to three “empirical arenas” (Fine 1993:61) are examined: the production of identities, the sociology of emotion, and the construction of social problems. In each of these areas, interactionists have emphasized the importance of definitional processes.

### 2.2 Symbolic Interactionism’s Premises

Expanding upon Mead, Blumer (1938) is credited with coinining the term symbolic interaction. In the seminal work *Symbolic Interactionism*, he presented three premises: that individuals act based on the meaning of social objects, that meanings are constructed through social interaction, and that meanings are modified throughout processes of interpretation (Blumer 1969:2). Similar to other early contributions to symbolic interactionism, Blumer’s elaborations were positioned as defenses against and attacks toward functionalism (Colomy and Brown 1995).

Despite differences in emphases within symbolic interactionism, summaries and critiques of the approach prioritize Blumer’s premises (Dennis and Martin 2005; Fine 1993; Snow 2001). The tendency to begin summaries of interactionism with Blumer’s three premises, as done here, emphasizes certain interactionist concepts while neglecting others, which may account for some

---

³ Sensitizing concepts refer to those that provide guidance for areas of inquiry and examination, but that do not have concrete definitions (Blumer 1954). Many sociological concepts are sensitizing in nature, including class, structure (ibid), labels, and emotions.
common misconceptions about interactionism⁴ (Snow 2001). More recently, contributions to interactionism have emphasized different principles to capture the broader framework presented by Mead and Blumer. The refocusing of emphasis also addresses popular distortions and critiques of interactionism such as the charge that it is limited to ‘micro’ analyses. In fact, interactionism is suited for the study of institutions and institutionalized action (see Athens 2005; Maines 1977) and Mead (1934, 1936) explicitly addressed the creation and reformation of institutions as well as their role in organizing social action.

Snow (2001:368) supplemented Blumer’s premises by outlining four principles of symbolic interactionism: interactive determination, symbolization, emergence, and human agency. These principles align with three “orienting propositions” of interactionism identified by Maines (2001:3-4, 2003): that society and individual are inseparable parts of the same process, that human action involves meaning exchanges, and that change is inherent to sociality.

The principle of interactive determination asserts that studying the qualities of groups, phenomena, or individuals cannot be accomplished without examining the relationships and interactions within which they are embedded (Snow 2001). Similarly, society and self exist only in relation and cannot be separated to give either primacy (Athens 2005; Snow 2001). As Maines (2001) noted: “individuals are always social beings, and societies are always composed of interacting individuals” (p. 4).

---

⁴ For example, Blumer’s premises focus on interpretation and meaning. The failure of interactionist studies to foreground social organizations may play a role in the common misconception of symbolic interactionism as a ‘micro’ perspective (Snow 2001:368).
The principle of *symbolization* is captured by Blumer’s three premises and refers to the process through which groups, events, and other phenomena become social objects that are connected to meaning (Maines 2001, 2003; Snow 2001). Blumer’s summary illustrates the active role of individuals’ interpretations of symbols. Snow (2001) challenged that this may over-emphasize the active element, as some actions are routinized without continuous interpretation and reflection. Similarly, Shibutani (1961) asserted that active interpretation and consciously planned actions occur more often during novel, rather than routine, situations. Finally, in presenting a ‘radical’ interactionism, Athens (2007) argued that even sub-ordinate and super-ordinate roles in joint action can be routinized rather than actively reflected upon. As such, examining the processes through which meanings become taken-for-granted is a necessary sociological pursuit (Snow 2001).

The principle of *emergence* reflects symbolic interactionists’ interest in novel phenomena, including changes in identity, joint actions, behaviors, definitions (Snow 2001), and institutions (Athens 2005). As Maines (2001) argued, “variation, change, and uncertainty are intrinsic to human group life” (p. 4). Although emergence was not specifically articulated in Blumer’s (1969) premises, he described this principle eight pages later: “by virtue of symbolic interaction, human group life is necessarily a formative process and not a mere arena for the expression of pre-existing factors” (p. 10).

The principle of *agency* reflects an understanding that human actions are not predetermined as individuals are active in their environment (Snow 2001). Since Mead (1922, 1934), interactionists have acknowledged that although a variety of factors influence the pursuit of action, individuals must be understood as active rather than passive. Further, although social
constraints may be taken-for-granted and actions routinized, the agentic nature of humans is most evident when individuals face novel circumstances (Snow 2001).

2.3 Selves, Identities, and Roles

The concept of the self has garnered significant attention by interactionists. Like other social objects, the self is seen as a process that is continually shaped and reshaped throughout interactions (Blumer 1969; Mead 1934). The self is inherently social and is both a product of interactions and a factor influencing choices in actions (Rock 1979; Rosenberg 1981). The uniqueness of the self as a concept is that it can be “object to itself” (Mead 1934:136), meaning that it originates in interaction much like any object that can be referred to (Shibutani 1961). Although a minority of symbolic interactionists view the self as relatively stable based on the networks within which one interacts (Kuhn and McPartland 1954; Stryker 1980, 2008), most interactionists see the self as continuously adjusting its presentation and meaning (Mead 1934; Rosenberg 1981).

While interactionists agree that some identifiers of the self are given more primacy than others, there is no consensus on the definition of social identities (Rosenberg 1981). Aspects of identity include social statuses, membership groups, labels, and types (ibid:602). These elements – from gender to religion to deviant status to self-labeling as antisocial – impact self-conception and, in turn, future actions (ibid).

Role-taking is a distinct human ability, made possible through symbols and language, which allows for the imagination of others’ attitudes and perspectives. Mead (1934) conceptualized the generalized other as the attitudes of the community, which enables thinking and conceptualizations of the self. Blumer (1938) expanded that most changes in self-
conceptions reflect new views of the generalized other. The ability to assume the attitudes of others is also an important mechanism of social control: “self-criticism is essentially social criticism, and behavior controlled by self-criticism is essentially behavior controlled socially” (Mead 1934:255).

The concept of reference groups emphasizes that social actors can take the role of specific groups when thinking about the self, rather than the abstract attitude of the entire community (Shibutani 1961). Using certain groups as frames for role-taking, reference groups can increase conformity or differentiation (Singer 1981). This concept further demonstrates the importance of role-taking to social control. During interactions with others, individuals evaluate the self as an object and monitor their behavior in terms of group norms (Shibutani 1961).

In proposing a radical interactionism, which further emphasizes power in relationships and interactions, Athens (2007) replaced the concept of generalized other with phantom communities. Although conceptually similar, phantom communities account for the tendency of individuals to take the attitudes of others for granted (ibid). When the attitudes of parents, teachers, employers, and others in superordinate roles are considered regularly, subordinate roles can become routinized (ibid). Therefore, the concept of phantom communities reflects how social control can become taken-for-granted over time (ibid).

Through the roles one assumes, self-conceptions can influence choices of actions. When joint action is undertaken, participants come to expect other actors to perform specific actions. A role thus refers to the expected pattern of behavior based on the institutionalization of joint action (Athens 2005) and reflects norms in group life (Shibutani 1961). Roles could include anything from a home-plate umpire in a baseball game, to an attendee of a Catholic church, to
the eldest child in a family. Individuals are usually members of multiple social groups and may hold different roles in each (Park [1929] 1952). While self-conceptions influence the roles taken in institutionalized social acts, performance in those roles can further shift or reinforce self-conceptions.

Scholars have also attended to the relationship between online arenas and the self. A primary focus for those studying the self online has been how individuals present on the internet as opposed to how they conceive of themselves following online interactions (Zhao 2011). Interactionist contributions to understanding the self online have typically involved extending interactionist concepts to online contexts (Hogan 2010; Robinson 2007). For example, Robinson (2007) extended Mead’s generalized other to account for how individuals may take the role of particular online communities when examining the self as object, where norms may differ significantly from offline expectations.

Holstein and Gubrium (2000) emphasized that contemporary technological landscapes provide more contexts for processes of self-identification and construction. However, in contrast to some claims that the postmodern self has lost its individuality through increasingly immediate communication, changing technological landscapes have merely produced more contexts in which the self can be displayed, constructed, and conceived (ibid). As Zhao (2011) noted, even though the World Wide Web enables global connections in countless different forms, the places we visit and people we connect to online are just as, if not more, self-selected than offline. Finally, a significant element of these applications for interactionist research in online spheres is the extension of the concept of co-presence to online arenas. Campos-Castillo and Hitlin (2013) defined co-presence as the subjective experience of mutual attention to account for technologies
that can substitute for physical co-presence. Accordingly, interactions and identity processes online can be understood to function similarly to offline.

2.4 Self-Labeling and Becoming

Based on the preceding discussion, an important area of interactionist analysis of the self involves the emergent processes of identities, including changing self-conceptions and the implementation of new self-labels. This is central for theoretically informing this study’s research question about whether individuals come to see themselves as victims. Further, self-conceptions are likely to inform choices in action and may therefore influence identity theft victims’ reporting decisions.

Due in part to victimology’s positivist origins, relatively little research has focused on the changes in self-conceptions involved in becoming a victim. The contributions to self-changes have typically stemmed from research on violence against women. These discussions include arguments concerning the role of external definitions in problematizing violence and the importance of interpretive environments that present rationalizations for explaining violence (Ferraro 2006; Ferraro and Johnson 1983). When these rationalizations are contested, changes in self-definition may result in victims defining their relationships as problematic and themselves as victims (Dunn 2008). Although there are few discussions of self-definition processes among victims, deviance scholars have presented major contributions to interactionist understandings of changes in self-conceptions. While becoming deviant no doubt represents a different substantive focus than becoming a victim, the process of changing one’s self-conception by drawing on interpretive environments, reference groups, and social others is theoretically analogous (Matza 1969).
Labeling theory (Becker [1963] 1973; Lemert 1951; Schur 1971) is an interactionist theory of deviance whose proponents contend that deviance results from societal reactions rather than some inherent quality of individuals. The discussions by labeling theorists have elucidated the relationships between societal reactions and self-perceptions. Lemert’s (1951) differentiation of primary and secondary deviance highlighted processes of accepting new roles and self-definitions. Primary deviance is defined as any act described as deviance by others but that the actor rationalizes as normal, while secondary deviance refers to those acts defined as deviance which result from a previous societal reaction (ibid:75-6). Thus, secondary deviance can involve an actor embracing a deviant role, which Lemert (1951) argued is the most sociologically important form of deviance. Such redefinition aligns with interactionist views of the self, where the perceptions of others constitute an important component of self-conceptions. Matsueda (1992) demonstrated the importance of role-taking to self-labels by conceptualizing “the self as reflected appraisals” (p. 1603).

Becker ([1963] 1973) also discussed that while labels reflect external definitions of the rule-breaker, they may similarly impact self-conceptions. When labeled, individuals may change the groups with which they interact, thereby further shifting self-conceptions (ibid). Additionally, Becker ([1963] 1973) argued that a labeled individual “may himself act as enforcer” (p. 31) by altering their self-image and acting in distinct ways based on the anticipated reactions of others. Similarly, Goode (1975) contended that many deviants can self-label based on anticipated reactions, suggesting that social reactions are not always necessary for changes in self-conception.
Link (1987) and Link et al. (1989) modified Becker’s contributions to examine the self-enforcement of labels by patients diagnosed with a mental disorder. They contended that prior to labeling, individuals are typically socialized in ways that present negative views of individuals with mental disorders (Link 1987). These conceptions may be modified and take on new relevance over time. When an individual is labeled, behaviors can change for two reasons. First, people may devalue themselves and identify with a negatively perceived group (ibid). Alternatively, the labeled individual may change their behavior while implementing defense mechanisms to avoid negative societal reactions, which may create further interactional issues (ibid). Significantly, Link (1987) and Link et al. (1989) argued that individuals are socialized to hold meaning for a social label – be it deviant, mentally ill, or victim – which takes on new meaning and relevance when the individual is so labeled. In turn, individuals may embrace or resist such labels depending on their personal experience with the label and based on their socialization with the phenomena of relevance.

The external application of a label does not necessitate a change in self-conception or determine future behavior. Paternoster and Iovanni (1989) emphasized that this process is equivocal: “given the occurrence of a labeling experience, the individual may experience an alteration of personal identity, may find access to conventional others and opportunities barred, and as a result may exhibit a greater involvement in deviant behavior” (p. 381; emphasis added). Similarly, Matza (1969) emphasized the importance of actors in mediating processes of becoming. The symbols and meaning related to the specific label embraced are central, as “the subject mediates the process of becoming in the terms and issues provided by the concrete matters before him” (Matza 1969:142; italics in original). Whether one who experiences the
misuse of their identity comes to self-label as a victim of identity theft is similarly equivocal due to the potential influence of external definitions and pre-existing conceptions about crime, victims, and identity theft.

2.5 The Symbolic Interactional Nature of Emotions

Emotional reactions to criminal victimization are common and past research suggests that fraud victimization may elicit unique emotions such as embarrassment and self-blame (Cross 2005). It is likely that these reactions influence victims’ actions in the aftermath of incidents. Although largely neglected in sociological thought, several symbolic interactionists have been analyzing emotions since the 1970s (Sandstrom and Kleinman 2005). Some sociologists distinguish emotions, affects, and similar terms in part to delineate the boundaries of sociological and psychological studies of emotions5 (see Franks 2003; Gordon 1981; Kemper 1978). Like Shott (1979:1318), these terms will be used to refer to similar phenomena, with emotions defined as aroused states that the actor identifies as emotionally induced. Interactionists do not deny the physiological elements of emotion (Fields et al. 2006; Shott 1979) but emphasize the necessary condition of an actor defining the perceived arousal as emotional. Shott (1979) summarized the emergent and precarious interactionist view of emotions as follows:

Within the limits set by social norms and internal stimuli, individuals construct their emotions; and their definitions and interpretations are critical to this often emergent process. Internal states and cues, necessary as they are for affective experience, do not in themselves establish feeling, for it is the actor’s definitions and interpretations that give physiological states their emotional significance or nonsignificance. (P. 1323)

5 “Sentiment” is another similar concept worth differentiating. Shibutani (1961) used the term to denote the attitude an individual holds toward another individual. Some scholars studying emotion use the concept similarly to describe attitudes that relate to social symbols of emotion, such as love and hate (see Gordon 1981; Thoits 1989).
Interactionism is beneficial for studying emotions as they are socialized, constructed by actors, and managed by individuals in interactions (Shott 1979). First, because emotions are socialized differently across cultures, the study of emotions is of sociological interest. Within society, emotions are differentiated to establish definitional boundaries and are socialized to become interpretive references for actors (Gordon 1981). Accordingly, the meaning, display, and situational appropriateness of emotions varies across social contexts (Gordon 1981; Shott 1979).

Second, emotions are not predetermined by physiological arousal, but are instead interpretively mediated by the actor (Gordon 1981). As interactionism focuses on the construction of meaning through symbolization, it is well-equipped to study emotions, which arise through this emergent process (Fields et al. 2006; Shott 1979). Athens (1994) argued that emotions are made possible through the ability to soliloquize by having a dialogue between the self and imagined others. To modify Matza (1969), if processes of becoming a new identity are mediated by the actor, so too are processes of becoming emotional.

Third, interactionism is useful for studying the management of emotions in interactions. Throughout interpersonal interactions, actors manage their emotions as well as the emotions of others (Goffman 1952, 1956). For example, Francis (1994) examined how humor can be used in interactions to generate positive attitudes when faced with a negative threat. Further, emotions can be regulated by groups and institutionalized norms (Gordon 1981). Hochschild (1979, 1990) discussed feeling rules as institutionalized guidelines for how individuals are expected to affectively feel and behave. In sum, due to the socialized, actively constructed, and managed nature of emotions, interactionism is well-suited for their study.
Further, some interactionists have argued that studying emotions is necessary for sociologists to fully understand society (Fields, Copp, and Kleinman 2006; Franks 2003; Sandstrom and Kleinman 2005; Shott 1979). Franks (2003) argued that studying emotion is paramount for symbolic interactionists as the focus on language and meaning requires an understanding of emotions. Further, although early interactionists identify that role-taking enables social control, this function would be ineffective without emotions such as shame and embarrassment (ibid). Finally, studies of emotion can provide deeper understandings of a variety of social relationships, including inequalities (Fields et al. 2006), interactional dynamics (Goffman 1956; Gross and Stone 1964), and the relationship between self and society (Goffman 1952).

2.6 Role-Taking Emotions

Role-taking emotions are those that involve assuming the perspective of others. They are relevant for interactional analysis as they involve self-monitoring and social control, and they influence social action (Thoits 1989). Despite paying little attention to emotions, Mead (1934) used the term role-taking to refer to assuming the attitudes of others during interactions. Cooley ([1902] 2009), who shared Mead’s view of society and self as co-constituted, introduced the looking-glass self to highlight how individuals continually self-monitor based on the anticipated evaluations of others. He argued that role-taking can result in evaluations of the self that lead to feelings such as shame and pride (ibid).

Amidst sociology’s increased interest in emotions in the late 1970s, interactionists emphasized the importance of role-taking to emotions. Shott (1979) described a subset of emotions, including pride, shame, embarrassment, and guilt, as role-taking emotions, which
necessarily involve viewing the self from the perspective of others. Similarly, Kemper (1978) argued that “a very large class of emotions results from real, imagined, or anticipated outcomes in social relationships” (p. 43). Thus, although some role-taking emotions such as embarrassment may be most likely to occur in interactions or groups, they can arise regardless of the presence of others (Scheff 1988, 2000; Shott 1979).  

Role-taking emotions are significant mechanisms of social control, as individuals act, in part, based on emotional reactions to viewing the self from the perspective of others (Shott 1979). Although the ability to take oneself as object and adjust based on the views of others has always been a notion in interactionism (Mead 1934:255), Shott (1979) contended that role-taking and social control impact social action because of the emotions they elicit.

Embarrassment and shame have received sociological attention due to their importance in social control (Cahill 1995; Gross and Stone 1964; Modigliani 1968; Scheff 1988) and tendency to demonstrate underlying dimensions of interactions (Gross and Stone 1964). Scholars have tended to focus on negative consequences of embarrassment and shame in disrupting interactions and damaging roles (Modigliani 1968), self-conceptions (Goffman 1952), and social bonds (Scheff 2000). Nonetheless, Cahill (1995) contended that positive consequences of embarrassment such as trust, self-regulation, and the reinforcement of norms must also be considered.

Role-taking emotions are precarious and can arise throughout most interactions. Embarrassment can result from missteps based on roles (Modigliani 1968), identities, or groups

6 The likelihood and manner of displaying role-taking emotions are also likely to vary across culture (see Markus and Kitayama 1991).
In turn, the constant risk of embarrassment or missteps influences choices of action (Cahill 1995; Goffman 1959). While Modigliani (1968) originally used the term embarrassability to discuss individuals’ differential capacities for becoming embarrassed, Cahill (1995) used it to demonstrate that “the ubiquitous possibility of embarrassment clearly constrains most of us much of the time” (p. 258). Embarrassment is not unique among role-taking emotions in its importance, as Scheff (1988) argued that people are almost always in some state of shame or pride, while Franks (2003) observed that pride is common when acting in roles that align with self-conceptions. As such, because of humans’ social nature and ability to take the self as object, role-taking emotions are common, with attitudes about which actions are embarrassing or shameful learned through social interactions and varying based on social context (Gordon 1981).

Individuals’ choices of actions are often informed by the potential for missteps, embarrassment, and shame. For example, embarrassment and shame are likely to be relevant to choices of actions in the aftermath of victimizations that are viewed as preventable (see Cross 2015). Some of those actions are management strategies, including carefully discerning what and to whom information is disclosed (Goffman 1963). Most individuals use tact to avoid putting others in embarrassing situations, but interactions with actors who fail to use tact may influence the choices of what to disclose and from whom to seek help (Goffman 1956, 1967).

Goffman’s (1952) discussion of frauds that trick targets is especially relevant to the relationship between emotion, views of the self, and social action. During the preliminary stages of these frauds, perpetrators work to convince potential victims that they are making a smart decision, resulting in a destruction of self-conception when the victim realizes that they have
been tricked (ibid). The perpetrator or an accomplice to the fraud often influences victims’ choices in the aftermath by presenting rationalizations on which the victim can draw (ibid). Similarly, stalling is a tactic that prevents the victim from identifying the perpetrator, thus defusing any possible anger and leading to a decreased likelihood of the victim retaliating (ibid). The influence of identifying a perpetrator on reporting decisions will be discussed in the context of identity theft victims in the subsequent chapter.

2.7 The Construction of Social Problems

Scholars have yet to attend to how citizens understand identity theft as a social problem in contemporary society. Victims’ understandings of identity theft inform their responses in its aftermath. With research finding low police reporting rates by identity theft victims, it remains unclear whether the general population views identity theft as a serious social problem meriting attention or accepts it as an inevitable consequence of technological innovations. Further, according to Link (1987) and Link et al. (1989), victims of crime are likely to compare their experience to their prior understanding of the social problem.

In the 1970s, interactionists examining social problems called attention to objectivist assumptions in dominant sociological approaches. Similar to labeling theorists, interactionists studying social problems attend to definitional processes. Prior approaches to social problems assumed that the problems studied were objective conditions to be solved (Blumer 1971; Spector and Kitsuse [1977] 2009). Now known as constructionism, Spector and Kitsuse’s ([1977] 2009) interactionist-based approach to social problems examines claims-making, a specific form of social activity. The constructionist approach to social problems encompasses interactionist
principles by understanding social problems as emergent, symbolic, and interactionally
determined.

Blumer (1971) noted the inadequacy of prior approaches to social problems which
simultaneously treated social problems as objective while neglecting the social processes through
which these issues garnered sociological attention. Early social problems researchers labeled the
phenomenon of study as pathological, then sought to identify its causes in order to provide
solutions (ibid). Objectivist approaches ignore conflicting claims made about social problems,
and Blumer (1971) instead suggested that “social problems lie in and are the products of a
process of collective definition” (p. 301).

Spector and Kitsuse ([1977] 2009) defined social problems as “the activities of
individuals or groups making assertions of grievances and claims with respect to some putative
conditions” (p. 75). They rejected objectivist claims that view social problems as conditions of
societies. Instead, analyses of social problems should focus on the interactions between groups
making claims “regarding the definition of social conditions” (ibid:72). As such, Spector and
Kitsuse ([1977] 2009) contended that analyses of social problems should examine the claims
made about alleged problems rather than take as their starting point the view of social problems
as real and requiring solutions.

Debates within the sociology of social problems stem from Woolgar and Pawluch’s
(1985) charge of “ontological gerrymandering,” which is the practice of setting boundaries that
determine which phenomena are problematized in an analysis. In definitional approaches to
social problems research, the competing claims about a problem are questioned and analyzed
while the problem itself is often treated as an objective condition of a society (ibid). For
example, when analyzing temporal changes in definitions of an alleged condition, scholars have tended to assume the condition itself has gone unchanged over time (ibid:216). In the case of identity theft, statistics often emphasize increasing rates (Harrell 2019) without discussion of the emerging and shifting forms of incidents included within definitions of identity theft. Woolgar and Pawluch (1985:224) acknowledged that ontological gerrymandering can be viewed as either a significant inconsistency or an inevitable practice in social problems research.

This resulted in the identification of three approaches to constructionism: those debunking claims, strict constructionists, and contextual constructionists (Best 1989). First, some scholars identifying with constructionist orientations are guilty of ontological gerrymandering when approaching a social problem with the aim of “debunking” claims (ibid:246). Critics argue that to disprove a claim about a social problem implies an objectivist reality.

Strict constructionism is most concerned with avoiding ontological gerrymandering. Kitsuse ([2000] 2009) contended that their view of the sociology of social problems did not require evaluating social conditions as valid or real. Instead, Ibarra and Kitsuse (1993) argued that the study of social problems can focus exclusively on the claims made about conditions. In contrast, Best advocated for contextual constructionism, which maintains a focus on claims-making but “acknowledge[s] making some assumptions about social conditions” (Best 1989:246). For example, contextual constructionists, unlike strict constructionists, may compare claims made about social phenomena to other social information, such as crime rates (ibid:247). In this approach, scientific contributions, official statistics, or victimization survey results could be viewed as other forms of socially constructed data that are open for evaluation (ibid).

Interactionists have long acknowledged the importance of language as a primary social
institution (Mead 1934) and Best (2003) observed that “in practice, analysts’ dependence on language – itself embedded in a social context – ensures that any sociological analysis must be founded on some assumptions about social life” (p. 984).

Gusfield, who Best identified as a contextual constructionist, argued that it is uncertain whether ongoing debate about ontological boundaries is beneficial as it fails to contribute to empirical findings (Gusfield 1985 cited in Best 1993). Whether one analyzes social problems by evaluating claims or official statistics, the analyses performed and data examined are socially constructed in the sense that they result from social action (Best 1989; Maines 2001). Amidst this long-lasting debate, Spector (2018) has recently suggested that scholars stop dwelling on philosophical dilemmas and instead focus on the definitional processes and tools suiting substantive inquiry. Regarding this critical literature, Spector (2018) suggested to young social problems researchers: “Do not waste too much time reading it. Do not contribute to it… Do not try to resolve the disagreements” (p. 180).

The processes through which social problems develop have been subject to debate with several scholars presenting natural histories of social problems (Spector and Kitsuse [1997] 2009). Blumer (1971) outlined that contingencies may occur throughout the emergence and legitimation of social problems as well as through the formation and implementation of suggested solutions. Spector and Kitsuse ([1997] 2009) argued that even after these stages, it is necessary to examine the consequences and counterclaims following the implementation of plans. In the case of identity theft, despite Canadian Criminal Code modifications reflecting the implementation of plans to address identity theft (Bill S-4 2009), it remains unclear under what conditions such plans are enacted. Further, the solutions presented for a social problem may
cause new social problems to emerge (Spector and Kitsuse [1997] 2009). This observation was expanded upon by Fine (2006) in his discussion of the “chaining of social problems,” whereby the implementation of plans is understood to impact the institutions and social relations of society. As such, solutions to social problems can present new issues communally defined as problems or can motivate claims-makers to draw attention to further issues (ibid).

The claims made about identity theft as a social problem inform how citizens understand the phenomenon and its victims. These prior conceptions act as an interpretive resource when having one’s identity information or account misused, thus impacting the choices individuals make in identity theft’s aftermath and their expectations of the various institutions involved.

2.8 Social Problems and Identities

Constructionist approaches can elucidate how individuals think about social problems. As it pertains to emerging crimes, Best (1999) argued that new crimes are institutionalized through mass media, governments, activists, and experts, with new victims emerging simultaneously to new crimes. Although much attention is devoted to analyzing original claims about social problems, one can also analyze secondary claims disseminated through media or even tertiary claims by ordinary citizens (Best 2003). While media are certainly important for informing peoples’ understandings of crimes and social problems (Best 1999; Rock 2002), Sasson (1995) encouraged scholars to examine the actual understandings citizens hold about crime rather than forming assumptions based on media depictions. Sasson’s examination of “crime talk” found that individuals draw on a combination of their personal experiences with crime as well as frames presented in media depictions (ibid).
The processes of becoming and self-labeling, discussed in Section 2.4, often relate to social problems construction. Generally, victim identities relate to social problems construction in several important ways. Claiming an identity or coming to see oneself as a victim involves interpretations of social problems and victimhood. Rock (2002) defined ‘victim’ as an identity dependent on a variety of individuals, including politicians, media, law enforcement, and others, “who may not deal with the individual case but who will nevertheless shape the larger interpretative environment in which it is lodged” (p. 15). In this sense, victimhood emerges from interactional processes despite being commonly viewed as a clear-cut identity (Holstein and Miller 1990). Similar to the labeling work by Link (1987) and Link et al. (1989), individuals have existing attitudes toward identity theft and its victims, which may take on new meanings when faced with a potential victimizing event. Along with rationalization processes (Bograd 1998; Ferraro and Johnson 1983; Mills 1985) and external definitions by significant others (Ferraro and Johnson 1983; Loseke 1992, 2001), the production and reproduction of claims about social problems influence whether one will identify as a victim.

Imagery of typical victims represents another way in which identities relate to social problems. A main tactic in claims-making about social problems is to identify victims and garner sympathy to illustrate the condition’s impact (Dunn 2008). Further, Christie (1968) described ideal victims as individuals who “most readily are given the complete and legitimate status of being a victim” (p. 18). Although the characteristics defining ideal victims vary based on social context, they are often tied to conceptions of innocence. Best (1999) argued that the “contemporary ideology of victimization” (p. 103) includes understanding victimization as straightforward and unambiguous. In practice, the experiences of victims are more complex and
rarely align with depictions of ideal victims, which can have consequences for the societal reactions to the victim and to the assistance they receive from others (Hoyle, Bosworth, and Dempsey 2011; Leisenring 2006; Loseke 1992). For example, Loseke (1987) argued that wife abuse as constructed by official definitions and claims-makers rarely matches the experiences of those victims seeking support from shelters, which may impact whether they receive help. Of the women who enter the shelter, Loseke (1987) asked: “did they each understand themselves, their partners, and their experiences in terms of official definitions?” (p. 236). Of course, this question could also be posed to those victims who do not seek institutional assistance in the aftermath of a crime. In the case of identity theft, it is possible that many victims fitting formal definitions find a disjuncture between their experiences and their prior conceptions of what constitutes an identity theft victim, thus impacting their self-perceptions and choices in the aftermath of identity theft. The relatively little research that has examined perceptions of identity theft and its victims will be discussed in the literature review.

2.9 Summary

Interactionist contributions to the study of identity formation, emotions, and social problems provide a number of sensitizing concepts to begin inquiry into an under-researched social phenomenon such as identity theft victimization. Victimhood refers to an identity or role with which individuals fitting legal definitions as victims may or may not align. Resistance to or acceptance of the victim identity may relate to societal depictions surrounding the symbols of victims and survivors.

Emotions, understood as definitional reactions to perceived stimuli, are important to processes of becoming as well as to choices of action. Many of the most sociologically relevant
emotions involve role-taking, which result from self-evaluations from the perspectives of others. An individual’s identification with particular emotions may subsequently influence their behavior and choices of interactions. For example, fraud can elicit role-taking emotions such as embarrassment, which sometimes influences victims to keep the incident to themselves (see Cross 2015).

Finally, choices of action, experiences of emotion, and acceptance of labels relate to peoples’ understandings of identity theft and its victims. In some instances, claims-makers emphasize the harm done to victims to raise awareness about a social problem. The claims made in media, news, television, advertisements, and elsewhere contribute to the knowledge on which individuals draw when confronted with a victimizing event.

Interactionism is beneficial to the study of social action for its emphases on symbolization, interactions, emergence, and agency. The following chapter will discuss substantive research regarding identity theft and fraud victimization, including victims’ reporting decisions and satisfaction with institutions in the aftermath of crimes.
3 Literature Review

3.1 Introduction

Identity theft is one of the fastest growing crimes in North America (Golladay 2020; Moreau 2021; Piquero et al. 2011). While many incidents are reported to financial institutions, few are reported to law enforcement (Harrell 2019; Sproule and Archer 2008) and thereby brought to the attention of authorities tasked with responding to and preventing them. Identity theft is used here to describe the combined acts of identity theft and fraud, where identity theft is the illegal theft or possession of identity information and fraud is the information’s misuse (McNally and Newman 2008). This study seeks to answer research questions about how victims conceptualize identity theft incidents and themselves, where and why they report incidents, and whether they are satisfied with the resolutions facilitated by responding institutions. This chapter situates this study within past research on victims of identity theft, fraud, and other crimes.

The chapter begins by providing legal definitions of identity theft in Canada and the United States and presenting prevalence estimates and common consequences of identity theft victimization. Next, it situates this study’s research questions within past research on identity theft and victims. First, it discusses the limited research that addresses victims’ experiences and perceptions of identity theft, cybercrime, and fraud and broader research examining the processes of becoming a victim. Following this, the chapter reviews past studies that have examined identity theft victims’ reporting decisions and then discusses research on victims’ satisfaction with institutions in the aftermath of identity theft and fraud.
3.2 Identity Theft Definitions, Prevalence Estimates, and Consequences

3.2.1 Identity Theft and Fraud

The definition of identity theft varies based on jurisdiction and can take on different meanings in scholarly and informal contexts. The term has existed for decades, yet recent expansions in technologies that facilitate identity theft have led to increased attention and changes to legal codes and definitions. Identity theft is often used to describe the combined act of the theft of identity information and its misuse; in most cases, the latter depends on the former (McNally and Newman 2008).

Identity theft began being criminalized in American states in the 1990s and in Canada a decade later (Archer et al. 2012), and these countries’ legal definitions of identity theft are similar. In both countries, identity theft refers to the possession or acquisition of another’s identity information with the intention to commit a crime (C.C.C., RSC 1985, c C-46: s 402.2; 18 U.S.C. § 1028A). In Canada, the term identity fraud is used to define the misuse of identity information for self-benefit or to harm another (C.C.C., RSC, c-46: s 403). The United States Code bans such fraud but does not use the specific term identity fraud (U.S.C. § 1028). Finally, while the United States Code describes identity information as any “means of identification of another person” (18 U.S.C § 1028A), the Canadian Criminal Code (RSC, c-46: s 402.1) specifies that identity information refers to anything that can uniquely identify another individual, from names, fingerprints, or signatures to passwords, passports, or credit card numbers.

Both the acquisition and misuse of identity information can occur online or offline. Common forms of acquiring identity information include hacking and phishing scams or
dumpster diving and stealing physical documents (Archer et al. 2012). The most common type of identity theft is the misuse of existing account information, including a bank, credit card, or other company account, and this constituted approximately 85 percent of identity theft victimizations in the United States in 2016\(^7\) (Harrell 2019:5).

Critical perspectives have identified definitional ambiguities surrounding fraud and financial crimes. Deem, Nerenberg, and Titus (2013) argued that there is a continuum of intentionally deceptive practices in modern society, where legal boundaries may not always be clear. They provided the example of free trials, where some companies make cancelling subscriptions difficult, hide agreement terms, or altogether misuse consumers’ personal information (ibid). Moreover, the forms of fraud that constitute identity theft regularly evolve, and new forms emerge. For example, phone porting scams are relatively novel and involve fraudsters illegally transferring a victim’s smartphone number to their possession to access associated accounts (Office of the Privacy Commissioner of Canada 2020).

Finally, some scholars have criticized the use of the term identity theft. For example, some have challenged the term since most of the crimes included are forms of fraud and not theft (Dupont 2012; Wall 2008). Moreover, Dupont (2012) observed that victims’ identities are seldom actually stolen; rather, a second person has access to identity information in addition to the victim.

\(^7\) The 2018 version of the NCVS – ITS was released after data analysis for this dissertation was complete. Because the 2016 edition was used for analyses, data from the 2016 Bureau of Justice Statistics report (Harrell 2019) is reported here; estimates from the 2018 iteration are comparable. For example, in both editions, when rounded to the nearest integer, 7 percent of victims reported to police, 88 percent to financial institutions, and 8 percent to credit bureaus (Harrell 2019:13-4, 2021:13-4).
For the purpose of this study and in line with both the NCVS – ITS and North American legal codes, identity theft refers to the combined act of identity theft and fraud. The NCVS – ITS includes in its sample victims who have experienced the misuse of an existing account, including bank, credit card, or other; the creation of a new account in their name; or another fraudulent misuse of their personal information⁸ (United States Department of Justice 2016). These inclusion criteria are described further in the Methods section and have implications that will be examined in the Discussion.

3.2.2 Prevalence

In the United States, the Bureau of Justice Statistics collects information on identity theft through the NCVS – ITS and found that 10 percent of adults were victimized in 2016 (Harrell 2019). In the United States, identity theft increased rapidly in the 2000s (Piquero, Cohen, and Piquero 2011) and victimization rates continued to rise from 2012 to 2016 (Harrell and Langton 2013; Harrell 2019). In Canada, there have been no recent representative surveys to estimate the prevalence of identity theft; the last identity theft victim survey was conducted by Sproule and Archer in 2008 and estimated that 6.5 percent of Canadian adults were victim to identity theft annually. This survey was collected before relevant revisions to the Canadian Criminal Code (Bill S-4 2009), and police-reported identity theft cases continue to increase (Moreau 2021).

Identity theft’s increase has been explained primarily due to changes in technology use in society, including the increased reliance on electronic payment systems (Anderson, Durbin, and Salinger 2008; Golladay and Holtfreter 2017). Brady, Randa, and Reyns (2016) argued that

---

⁸ Including having someone apply for government benefits in their name or impersonate them to a police officer or other authority.
increases in cybercrime, generally, are related to broader changes in online routines, and they found that increased national rates of online financial victimizations correlated with rises in internet use. At the individual level, Reynolds (2013) found that online shopping and banking predicted increased risk for identity theft victimization. Research has established that many identity theft victims are unsure how their information was obtained (Harrell 2019); thus, it remains unclear whether offline forms of identity theft are also increasing. Moreover, while identity theft is a staple of cybercrime discussions (see Wall 2008), the relative prevalence of online and offline forms of identity theft is unknown.9

In addition to increased internet and electronic payments, legal changes themselves may also contribute to perceptions of rising rates of identity theft. For example, Cole and Pontell (2006) argued that identity theft’s increasing prevalence was the result of both technological changes affording new opportunities and the legal changes that redefined existing forms of fraud as identity theft.

3.2.3 Consequences

Most victims of identity theft recuperate losses by contacting financial institutions or other companies (Copes et al. 2010), leading to misconceptions of identity theft and fraud as victimless crimes (Button, Lewis, and Tapley 2014; Cross 2018a). Instead, consequences of

9 Steinmetz and Nobles (2017) argued that the term "cybercrime" presents technologically related crimes as objective phenomena. This language tends to simplify complex social, technological, and definitional processes (ibid) and often presents online versus offline as a clear distinction. In the current context, scholars have often presented identity theft as a cybercrime by invoking an omniscient point of view, whereby the cause of the identity information’s theft and misuse are both known. In reality, many identity theft victims have little information about how their victimization occurred (Harrell 2019). Moreover, it is unclear whether victims of identity theft view the incidents as “cybercrimes.” As such, while I draw from contributions to cybercrime scholarship, I am resistant to describing identity theft as a cybercrime.
identity theft vary and can include losses of time and money, distress and, sometimes, relational and physical consequences.

Estimates from the 2016 NCVS – ITS suggested that two thirds (66 percent) of identity theft victims either had some amount of money, goods, or credit taken or paid fees as a result of the incident (Harrell 2019:8). The mean amount taken or lost before attempts at recuperation was $850 (ibid). In comparison, Sproule and Archer (2008) found that the average amount taken from Canadian victims was approximately $1100. Evidence from a 2006 Federal Trade Commission (FTC) dataset suggested that the amount taken by perpetrators varied based on the type of incident: victims of new account fraud and other fraudulent misuses of their personal information had mean amounts taken of $1350, while existing account frauds averaged less than $500 (Synovate 2007).

Twelve percent of American identity theft victims pay out of pocket after recuperation attempts, including for the direct amount taken and for indirect charges or fees (Harrell 2019). Based on prevalence estimates, this suggests that over 3 million Americans suffered out-of-pocket losses as a result of identity theft in 2016 (ibid). These victims lost an average of $690 when including those paying minor fees, with a median loss of $100 (ibid). When excluding those paying only indirect fees, victims suffering out-of-pocket losses had a mean loss of $841, with half of those victims losing over $200 (Reynolds 2021). As a result of the financial costs of identity theft, the American Identity Theft Resource Center (2018) found that some victims had to borrow money, sell possessions, or delay educational opportunities to recover from incidents.

Identity theft incidents can be resolved in as little as one phone call or can take months or years to correct. In 2016, the average American victim of identity theft spent four hours
resolving the incident, with over half of victims spending less than a day (Harrell 2019). In 2008, Canadians were estimated to spend an average of 13 hours resolving identity theft (Sproule and Archer 2008). Estimates of the time spent resolving incidents have varied significantly, either based on discrepancies in measures or in victim experiences (see Copes et al. 2010). For example, Pascoe et al. (2006) examined a sample of approximately 55,000 United Kingdom (UK) identity fraud victims and found a heavily skewed mean of 201 hours resolving incidents, despite 50 percent of victims having spent between 3 and 48 hours. Additionally, some American victims had to miss work or personal commitments due to the time spent resolving identity theft (Identity Theft Resource Center 2018).

Identity theft can also result in various emotional consequences. Pascoe et al. (2006) found that half of UK identity fraud victims reported that incidents had a considerable impact on stress or health, with repeat victims having experienced more stress. Further, in both the United Kingdom and the United States, increased time spent resolving incidents has been associated with elevated levels of victim distress (Harrell 2019; Pascoe et al. 2006). In the NCVS – ITS sample, many victims (46 percent) reported only mild distress from victimization (Harrell 2019:11). Nonetheless, almost all victims have reported some form of emotional consequence, including frustration, loss of trust, anger, and fear\(^{10}\) (Identity Theft Resource Center 2018). Additionally, Jansen and Leukfeldt (2018) found that victims of bank fraud that resulted from phishing scams often reported feeling stupid, ashamed, or embarrassed. At the extreme end,

\(^{10}\) Similarly, Abdulai (2020) found greater fear of future victimization amongst Canadian undergraduate students who had previously experienced debit or credit card fraud victimization.
Button et al. (2014) found that approximately 2 percent of UK fraud victims had considered suicide.\(^{11}\)

Although rarer, identity theft can also cause physical consequences, including headaches, difficulty sleeping, and pain (Golladay and Holtfreter 2017; Randa and Reyns 2020). Button et al. (2014:42) described that 11 percent of their UK sample reported some form of physical problem as a result of fraud. In these cases, physical symptoms were often psychosomatic, resulting from distress experienced (ibid).

Finally, some rarer consequences of identity theft and fraud include relational effects and unique secondary consequences. Of course, when one is victimized by someone they know, it is likely to impact their relationship. Relationships can also be affected in other ways: some victims have noted a lack of support from family and friends (Identity Theft Resource Center 2018), while victims’ families may experience increased financial and non-financial stress, including when victims keep fraud victimization as a secret (Button et al. 2014). Finally, other secondary consequences have been found to result from the credit problems associated with identity theft victimization, including difficulty renting housing or acquiring jobs (Identity Theft Resource Center 2018).

The consequences of identity theft vary even when situational characteristics of incidents are similar (Button et al. 2009; 2014). Studies drawing from American and Dutch samples have found that identity theft victims with lower incomes and lower educational attainment were more

\(^{11}\) Button et al.’s (2014) sample included all fraud victims. Although I do not know of notable cases covered by the media where identity theft led a victim to take their life, some exist for fraud more generally. William Foxton was a victim of Madoff’s Ponzi scheme and according to his family, he took his life as a result of the victimization (Satter 2009). Cross (2018a) also found that some victims of romance fraud expressed suicidal thoughts.
likely to suffer out-of-pocket losses than those with higher incomes and education (Reynolds 2021; van Wilsem, Sipma, and Meijer-van Leijsen 2021). Moreover, those who were unmarried had an increased likelihood of paying out of pocket in the United States (Reynolds 2021).

Relatedly, Deem (2000), who assisted victims of crime in the US Attorney’s office, found that consequences to financial crime victims often depended on their financial standing, where some victims did not have the resources to overcome the amount taken or the negative impacts to their credit scores.

In terms of emotional consequences, Pascoe et al. (2006) found that UK victims over 61 years old and those with higher incomes were less likely to report significant distress from victimization. Similarly, a Nigerian study of Automated Teller Machine (ATM) fraud found that distress depended on social support as well as life events (Tade and Adeniyi 2017). Thus, the consequences of identity theft and fraud vary not only based on situational factors but also based on personal characteristics and the support received from others.

In summary, identity theft and fraud are similarly criminalized in the United States and Canada and encompass a range of forms, including ones newly enabled by emerging technologies. The consequences of identity theft thus vary considerably. Although most victims recuperate financial losses, many face emotional costs, losses of time, and sometimes unique consequences.

3.3 Victims’ Experiences & Becoming a Victim

From an interactionist perspective, a victim’s understanding of identity theft and themselves is expected to inform their subsequent actions. However, few qualitative studies have attended to identity theft and research has yet to examine victims’ perceptions of identity theft.
incidents or their processes of self-defining in the aftermath. Nonetheless, contributions have come from discussions of identity theft victims and studies of the experiences of fraud and cybercrime victims as well as from critical contributions to victim research, including those studying violence against women. This section first examines research into identity theft victims’ knowledge about incidents, fraud victims’ experiences, and general perceptions of white-collar crime and cybercrime seriousness. Next, it discusses research that informs understandings of how individuals may come to see themselves as victims. Finally, it considers research that suggests that fraud victims are a stigmatized group, drawing from research into identity theft responsibility and victims’ and non-victims’ placement of blame.

3.3.1 Experiencing Identity Theft

Scholars have discussed whether victims who recuperate losses should be conceptualized as victims of identity theft. Koops and Leenes (2006) presented debates about definitions of identity theft victims and argued that since many victims recuperated losses, both the individual victim whose information was misused and the institution that suffered financial consequences could be viewed as a victim (ibid). In the latter case, the individual’s identity or account could instead be conceptualized as a tool used to victimize the institution (ibid). From this perspective, individual victims who lost money would be conceptualized differently from those who recuperated losses. Elsewhere, identity theft has been compared to the theft of keys\textsuperscript{12} since identity information is used to gain entrance to accounts where money, credit, or services can be

\textsuperscript{12} In fact, organizations could be conceptualized as victims in two ways: first, they could be victims of theft when organizations have been breached to access identity information, and second, they may be victims of fraud if identity information was misused to defraud accounts at those organizations (Green et al. 2020a).
stolen (Cole and Pontell 2006). However, scholars have argued that neglecting the individual victim because they usually recuperate losses is problematic, as many victims suffer non-financial harm (Golladay and Holtfreter 2017; Randa and Reynolds 2020).

If identity theft is like the theft of a key, it is unlike the theft of a house key that one would notice when they return home from work. Instead, most American victims discovered identity theft passively, including by being contacted by a financial institution (48 percent) or another company (5 percent), or after having charges or credit applications declined (6 percent; Harrell 2019:6). Only 27 percent of victims first discovered identity theft incidents by noticing charges on their account or realizing that money was missing (ibid). Accordingly, some victims may never notice an identity theft victimization or may notice it very late (Allison, Schuck, and Lersch 2005; Newman and McNally 2005), which suggests that some victims may never come to know an incident occurred and thus may never self-define as a victim.

Studies have found that emotional reactions are common immediately after discovering an identity theft incident. Following the public disclosure that hackers had accessed Equifax’s databases, the New York Times solicited victims of breaches to understand their experiences (Hsu 2017). While some victims discovered the breaches through such public disclosures, many found out passively after charges appeared, and these victims often described initial panic due to the uncertainty about whether other information had been stolen (Hsu 2017). Moreover, Green et al.’s (2020b) interviews with American identity theft victims found that many were caught off guard by their victimization, and fear, anger, and feelings of violation were common amongst victims.
Identity theft victims usually have limited knowledge about the incidents that took place. According to the 2016 estimates from the NCVS – ITS, almost three quarters (74 percent) of victims were unsure how their information was obtained, and even more (94 percent) knew nothing about their offender (Harrell 2019:7). Research from Australia found a similar trend, with most identity theft victims reporting that they were unsure how their information was taken, although many speculated possible means through which it was compromised (Turville, Yearwood, and Miller 2010). Many victims felt increased uncertainty and concern because they were unsure what other information the perpetrator may have accessed (ibid).

Some disparate studies have also informed this dissertation by providing insight into the processes and experiences of cybercrime and fraud victimization. Burgard and Schlembach (2013) examined victims of online scams, approximately one third of whom experienced fraud through Ebay. Borrowing from Goffman’s (1974) *Frame Analysis*, they argued that fraud and scam victimization have several stages (ibid). First, perpetrators isolate a victim and then decrease the level of precautions that the victim takes, allowing the perpetrator to trick the victim (ibid). In the final stage, the victim learns that they have been deceived and are victim to fraud, which often leads to rationalizing the experience given the new knowledge that they have been tricked (ibid). Goffman’s (1952) study of fraud interactions described a set of procedures that tricksters used in face-to-face interactions to cool the victim and attempt to prevent retaliation or help-seeking. Although Burgard and Schlembach (2013) described a fairly static procedure, some fraud victims may realize that a victimization occurred through a more dynamic process.

In the context of romance fraud, Cross and Layt (2021) found that nearly half of the potential victims that participated in their study had conducted internet searches to try to identify
the legitimacy of individuals with whom they were communicating. In some cases, these searches revealed to victims that the perpetrator was not legitimate and that they were being scammed (ibid). This suggests that the process of fraud victimization could involve multiple shifts in awareness if and when individuals realize that they have been victimized, how their information was obtained, or who their perpetrator was.

Finally, it remains unclear how citizens conceive of crimes like fraud and identity theft, although some studies have examined perceptions of white-collar crimes and cybercrimes. In academia, Sutherland’s 1940 presidential address to the American Society of Criminology criticized sampling bias in discussions of income and crime, where researchers consistently neglected white-collar crimes when presenting low income as a predictor for criminality. Additionally, while there tends to be consensus about the criminality of traditional interpersonal crimes, there is more variation in whether citizens perceive of white-collar crimes as crimes (Newman and Trilling 1975).

In the context of cybercrime, generally, Button et al. argued that victims’ experiences existed on a “continuum of impact” (2021:141) with three levels. Minor inconveniences were described as “everyday occurrence[s] to be expected in modern life” (ibid:141), where crimes of inconvenience were defined by victims as routine crimes, and serious violations were those considered to be significant offenses. Although none of these studies examined whether

---

13 However, there is reason to believe that fraud and identity theft may be normalized. For example, Cole and Pontell (2006) argued that the messaging surrounding identity theft is unlike that of other crimes, since it frames the crime as inevitable and places responsibility on individuals to protect themselves. This work is described further in a later section.

14 More recently, Green and Kugler (2012) found that American citizens usually identify white-collar crimes as criminal (including bribery, seller fraud, and perjury). In this case, participants provided binary closed-ended responses and the authors still found considerable variation across crimes (ibid).
individuals’ perceptions of crimes align with self-identification as a victim, it is likely that when criminality is ambiguous, so too is one’s victimhood.

3.3.2 Becoming a Victim

Although no previous research has examined whether identity theft victims view incidents as crimes or themselves as victims, some scholars have provided insights into these processes, generally. Most of these contributions come from research examining violence against women. Legally, a victim is defined in the Canadian Victims Bill of Rights as “an individual who has suffered physical or emotional harm, property damage or economic loss as the result of the commission or alleged commission of an offence” (2015:2). Still, victim statuses are often ambiguous (Christie 1986; Holstein and Miller 1990; Rock 2002), and, as Quinney argued, conceptions of victims are “optional, discretionary, and by no means innately given” (1972:314). As definitions of crimes vary across time and place, so too do definitions of victims and offenders (Christie 2004).

In fact, identifying as a victim may be more fluid than other identities, and individuals who could be defined as victims sometimes accept the label in certain contexts but resist it in others (Fohring 2018; Leisenring 2006). When a victim identity is accepted and applied by both the individual and others around them, it can invoke benefits in the form of sympathy, absolution of blame, or resources, including support, financial compensation, or goods (Dunn 2010; Rock 2002). Additionally, individuals can afford different priority to a victim identity: some may see it as a role they play in certain help-seeking contexts where others may incorporate it more centrally to their identity. In Canada, Kenney (2009) found that many individuals consulting victim support organizations did not initially identify as victims, based on their views of the
events as non-criminal or their perceived negative associations with the victim label. Related to the process of becoming a victim, scholars have examined how victimhood relates to awareness, external definitions, social conceptions of victims, and re-definitions of actions as problematic as opposed to normal.

First, becoming a victim relates to the victim’s awareness of the perpetrator’s behaviour. For example, a victim of theft may never realize their cash is missing. Similarly, identity theft victims may never notice that their accounts have been misused or that new accounts have been created in their names (Allison, Schuck, and Lersch 2005; Newman and McNally 2005).

In the context of studying interactions of dying individuals, Glaser and Strauss (1964; 1965) introduced the concept of awareness contexts. These refer to the possible combinations of knowledge that interactants have about one another (ibid). For example, both a patient and a doctor may know that the patient is dying, or a dying patient may suspect that they are dying but not tell their doctor, or vice versa. Regarding victims, Emerson, Ferris, and Gardner (1998) examined the process of stalking. They observed that in many cases, being followed is normalized for a period, but there is often a shift in the awareness context where the victim eventually realizes the extent to which the perpetrator is following them, leading them to problematize the actions or relationship (ibid). As such, becoming a victim may relate to the knowledge the victim has about the incident or the perpetrator’s actions.

Additionally, external definitions can influence self-identification as a victim. Loseke (1992) first examined how employees at women’s shelters assisted victims in redefining their experiences as abnormal. She argued that shelter employees’ priority was to assist women’s subjective transformations in problematizing violence and preparing for independence (ibid).
Through conversations, employees supported victims in understanding their situation as problematic and embracing the identity of a victim of abuse (ibid). Moreover, shelter workers tried to keep victims away from family members and friends who could have reinforced previous definitions of relationships or violence as normal (ibid). Later, Loseke (2001) examined the role of support groups for victims of abuse and found that many victims identified that employees’ external definitions informed their redefinitions of incidents. Finally, external definitions by others can undermine existing rationalizations of violence that victims use to normalize or downplay their situation (Ferraro and Johnson 1983; Mills 1985). Thus, external definitions can lead individuals to problematize actions against them and inform self-identification as a victim.

Scholars have also attended to the types of individuals most likely to be labeled as victims, such as Christie’s (1986) ideal victim, who is characterized as weak, innocent, and either young or old. Common depictions of weak and innocent victims have been important for advocacy groups in garnering victim support and generating consensus about social problems (Loseke 1992; O’Brien 2013). Nonetheless, this characterization of victims as innocent and passive has led to associations with weakness and powerlessness (Dunn 2010; Fohring 2018; Leisenring 2006), and some victims have resisted the label even when they accept that the incident that occurred was a crime (Fohring 2018). Moreover, the lived experiences of victims seldom align with depictions of ideal victims, which can create issues for receiving assistance from supporting institutions (Hoyle, Bosworth, and Dempsey 2011; Leisenring 2006; Loseke 1992).

Leisenring (2006) argued that victims of domestic violence are defined relative to public depictions of victims: “the assigning or claiming of a victim identity – and consequently, the
receipt of sympathy and assistance – is strongly tied both to existing public constructions of victims and to how individuals derive meaning from these constructions” (p. 309). Similarly, Loseke (2001) found that support workers often tried to align victims’ understandings of their experiences with common depictions of victims, which could help in redefining one’s experiences as problematic (ibid). She found that some victims resisted acceptance of these external definitions because they failed to see a parallel between their experiences and popular depictions of victims of violence (ibid).

Finally, there are many rationalizations that can impede understanding the self as a victim. Several scholars have drawn from Sykes and Matza (1957), who described techniques through which juveniles neutralized the effects of social control and justified delinquent acts. In the context of victimization, Dunn argued that to become a victim, women must first problematize their experience: “often, she must stop aligning and thereby neutralizing the behaviour of the person victimizing her in order to become a ‘victim’” (2008:1603).

Ferraro and Johnson (1983) modified Sykes and Matza’s techniques of neutralization and presented techniques through which victims rationalize domestic violence. Some of these techniques centered around the perpetrator, including rationalizing that the perpetrator needed help or that the harm was the fault of some external factor (ibid). Other victims denied that a victimization occurred by blaming their own actions for the incident or by refusing to acknowledge pain, injury, or harm (ibid). Finally, some victims denied that any alternatives existed or appealed to higher beliefs, insisting that the harm was worth it based on religious or personal beliefs (ibid). Similarly, Bograd (1998) maintains that violence is often rationalized through either excuses, which acknowledge the wrongfulness of the act but do not place blame
on the offender, or justifications, which downplay the act’s inappropriateness. Significantly, these rationalizations often relate to broader gendered stereotypes and inequalities that can be mobilized by perpetrators to maintain relational inequalities (Ferraro 2006; Sweet 2019). In these cases, when rationalizations are combatted and violence is redefined, individuals are likely to redefine themselves as a victim (Mills 1985).

The denial of victimization, or self-blame, has received attention from other scholars studying violence against women. Lempert (1994) performed a narrative case study of a woman leaving an abusive relationship, noting that she initially felt embarrassment over the incident before redefining the relationship as abnormal and the self as a victim. Similarly, Leisenring (2006) found that many women accepted some responsibility for the violence they experienced, which influenced their willingness to accept a victim label.

Victims of other crimes can also rationalize violence, and scholars have applied techniques of neutralization to other crimes, including elder abuse (Tomita 1990) and sexual victimization (Weiss 2011). For example, victims of sexual assault may deny harm when attempts at penetration are unsuccessful, may deny a victimization occurred when the victim is too drunk to stop the perpetrator, or may downplay the perpetrator’s intent when they are drunk or high (Weiss 2011). Similarly, elder abuse can be discounted by denying a victimization occurred because the elder committed some prior wrong (Tomita 1990). Moreover, harm can be

15 While techniques of neutralization and rationalization have not been applied to identity theft victimization, Copes and Vieraitis (2012) found that most identity theft perpetrators implement neutralization techniques, with over a third drawing from the denial of injury.
denied when physical consequences are downplayed or when financial exploitation is normalized based on the victims’ financial standing or the perpetrators’ future inheritance (ibid).

Finally, Brennan (2016) examined victims of violence, generally, and found that when perpetrators were friends, neighbours, or coworkers, victims were less likely to problematize the incidents or view them as criminal. Similarly, Burcar and Åkerström (2009) investigated how male victims of violence resisted or accepted the victim label and found that many argued the label fit them yet downplayed the harm experienced. Moreover, and tied to common depictions of victims, male victims often drew from common tropes of masculinity and resisted identification with the victim label by positioning themselves as acting bravely in the face of violence (ibid).

In summary, victimhood is often ambiguous, and even in cases where individuals fit legal definitions, they may not define themselves accordingly. Additionally, research rarely addresses whether definitions of events as crimes necessarily coincide with definitions of selves as victims. The studies informing this connection imply that individuals are more likely to view events as a crime and the self as a non-victim due to negative associations with the term (Fohring 2018; Leisenring 2006) than they are to view oneself as a victim while seeing events as a non-crime. From an interactionist perspective, this association depends on the meanings that crimes and victims hold for individuals and how these meanings align. Definitions of the self as a victim can involve comparisons to social depictions of victims and external definitions by loved ones and institutional actors. Moreover, rationalizations used to normalize behaviours or a lack of knowledge about incidents can act as barriers to defining the self as a victim.
3.3.3 Responsibility, Blame, and Stigma

Despite the limited research on identity theft victims’ experiences, some studies of identity theft and fraud victimization relate to the prior discussions of common depictions of victims and self-blame. Responsibility for identity theft protection has often fallen on individual consumers, which may relate to past research that has identified fraud victims as stigmatized (see Cross 2015).

Drawing on identity theft as a case study, Monahan (2009) argued that neoliberal discourses have framed protection against crime as an individual issue where potential victims are responsible for securing their information and data. Similarly, Cole and Pontell (2006) argued that the discourse surrounding identity theft has encouraged individuals to take responsibility for protecting their personal information and has masked the lack of effective official responses to rising cases of identity theft. This discourse may be somewhat unique to identity theft and fraud, since “media accounts of murder and robbery, for example, are not generally followed by a set of bullet-point recommendations for how the reader or viewer can avoid becoming a victim” (Cole and Pontell 2006:141).

Whitson and Haggerty (2008) similarly found that responsibility was placed on individual consumers in their study of North American law enforcement, government, and financial institutions’ identity theft messaging. Moreover, they observed that the protective measures recommended by these groups often exceeded reasonable expectations and neglected institutions’ roles in enabling many of the security risks from which consumers were expected to protect themselves. For example, advice from these institutions included shielding Personal Identification Numbers (PINs) from cameras positioned at ATMs and wiggling keypads to
ensure that they had not been tampered with (ibid). Cross (2017) observed that this notion of individual responsibility assumes citizens understand the risks involved with digital identifiers and ongoing technological change, which can be unrealistic for some groups, including seniors.

Although the reality is that anyone can be victimized, scholars have found that victims of fraud are often stigmatized (Button and Cross 2017). Cross (2015) interviewed Australian seniors, including both victims and non-victims who had received fraudulent e-mails, and found that victims were constructed as greedy and gullible. Notably, all of these victimizations involved tricking the participant into sending money or information to the offender, including phishing scams, advance-fee frauds, and romance frauds. In these types of incidents, victims are seen as having an active role in their own victimization, despite fraudsters using sophisticated tools and techniques (Cross 2015). For example, some fraudsters intentionally design scams to embarrass victims: romance frauds often involve tricking victims by using sensitive emotions and topics to make victims feel stupid or naïve (Button and Cross 2017). Nonetheless, this evidence suggests that victim-blaming discourses exist around fraud (Cross 2015).

Victim-blaming may also act as a barrier to help-seeking (Button and Cross 2017; Cross 2015). In Cross’s (2015) study, she found that those who responded to fraudulent e-mails often anticipated strong negative reactions from family and frequently used humor as a tool to distance themselves from perceived weakness. While many of the participants who did not respond to fraud attempts laughed at those who were scammed, even those who did respond used humour when describing other victims (ibid). Because of these attitudes, many victims internalized shame or embarrassment when disclosing or did not want to disclose their victimization (ibid). Moreover, Cross (2018b) found that fraud victims, who differed from depictions of ideal victims,
sometimes experienced trivialization of their circumstances by institutional actors and difficulty receiving benefits or recognition as a victim.

Burgard and Schlembach (2013) also observed self-blame in their study of online fraud victims. Several participants described feeling stupid for falling victim and others expressed anger with themselves (ibid). Moreover, while some victims who blamed themselves were able to seek help, others were more deeply ashamed and chose not to report the fraud to companies, law enforcement, or even friends (ibid). Although few identity theft incidents involve victims being tricked like in Ebay purchase scams, phishing scams, and romance fraud, this evidence suggests that fraud victims may generally be stigmatized.

In summary, identity theft victims’ experiences remain understudied, yet evidence suggests that few victims have information about their perpetrator or how they were victimized. Victims can learn new information about fraud incidents gradually, and online victimizations may be seen as serious crimes or minor inconveniences. Even when faced with incidents that can be legally defined as crimes, individuals may not self-define as a victim based on rationalizations, external definitions, their awareness of the incident, and common depictions of victims. Finally, research has found stigma surrounding fraud victims, whereby they are characterized as greedy or gullible, which can inform decision-making following victimization.

3.4 Victim’s Reporting Decisions and Experiences

Following identity theft, victims can report to a variety of institutions within what scholars have called “the fraud justice network” (Button, Tapley, and Lewis 2012:1). Unlike some crimes, identity theft cuts across sectors such that police do not have a monopoly on responding to these events. Instead, many companies, financial institutions, and support services
can also assist victims. Cybercrime scholars have argued that there is a new paradigm of security where numerous security actors must work together to respond to and prevent internet crimes (see Nhan 2010). After describing the recommendations to identity theft victims provided by the Canadian and United States governments, I will discuss past research into identity theft victims’ reporting behaviours and experiences with institutions.

The advice afforded to identity theft victims is different in Canada and the United States, with American victims facing more conflicting recommendations. Through online resources, the Canadian Government recommends that victims report incidents to both the local police and the Canadian Anti-Fraud Centre (CAFC), who are responsible for collecting data on fraud (Canadian Anti-Fraud Centre 2021). In the United States, the Department of Justice (2021) suggests that victims report to the companies where the fraud occurred, a credit bureau, the FTC, and then they may choose to report to local police.\textsuperscript{16} When identity theft was criminalized in the United States, the FTC was tasked with handling identity theft complaints and educating the public (Archer et al. 2012). The FTC created a website, identitytheft.gov, where victims can enter the details of the incident and receive advice regarding actions to take.

American victims also face several other reporting recommendations. Internet crimes, including identity theft, can be reported to the Federal Bureau of Investigation’s (FBI) Internet Crime Complaint Center (IC3; n.d), and the IC3 provide no indication of whether victims should report to one or both of the IC3 and the FTC. Finally, the Department of Homeland Security’s

\textsuperscript{16} Although the wording, ordering, and emphasis of these recommendations appear to have changed over time, archives of the webpage (through archive.org) reveal that these recommendations have existed since prior to July 2015.
(n.d.) website lists four official entities to which victims can report: the FTC, the IC3, a phishing scam reporting website, and the Social Security Administration for incidents involving Social Security Numbers (SSN). For example, if an American identity theft victim’s case involved the misuse of their SSN through a phishing scam, the advice would thus suggest that they report to these four institutions, along with other corporate or financial institutions where information was misused, a credit bureau, and, if they so choose, local police.

In their interviews with American identity theft victims, Green et al. (2020b) found that many victims were initially panicked and unsure of the correct course of action. Accordingly, victims often performed internet searches to try to discern what steps to take in the aftermath (ibid). Due to the differing recommendations, American victims may receive significantly different advice depending on the website reached or the keywords used.

3.4.1 Identity Theft Victim Reporting

The aftermath of identity theft is particularly understudied (Reyns and Randa 2017). In 2008, 54 percent of Canadian victims reported to credit card companies and 48 percent to banks, while only 13 percent reported to law enforcement and 6 percent reported to credit bureaus (Sproule and Archer 2008:25). In 2016, 7 percent of American victims reported to law enforcement, while 88 percent reported to credit card companies or banks and 8 percent reported to credit bureaus (Harrell 2019:13-4).

The perceived seriousness of an incident is the most common factor found to impact police reporting across crimes (Xie and Baumer 2019). In this sense, reporting is explained as a rational decision-making process based on the characteristics of the incident experienced (ibid). In the context of property crimes, multiple factors influence victims’ reporting, including
perceived seriousness, with an increased likelihood of reporting as greater amounts are taken (Greenberg and Beach 2004). Moreover, victims with heightened emotional reactions are more likely to report, as are those who receive recommendations to contact police\textsuperscript{17} (ibid).

Only two recent studies have examined the reporting decisions of identity theft victims, and the predictor variables they tested differed considerably. Reyns and Randa (2017) and Golladay (2017) each investigated identity theft reporting by drawing on the 2012 version of the NCVS – ITS. While Reyns and Randa (2017) examined reporting to police, Golladay (2017) also assessed reporting to financial institutions and credit bureaus.

Reyns and Randa (2017) identified several consequences that are similar to those that impact perceived seriousness for other crimes. They noted that research had not examined which factors impact victims’ perceptions of identity theft’s seriousness, although the amount taken, out-of-pocket loss, and physical and emotional distress were likely to play a role (ibid). Significantly, they found that suffering out-of-pocket loss increased the likelihood of reporting to police by approximately three times (ibid). Increased amounts taken by the perpetrator and longer duration of emotional distress also predicted reporting to law enforcement (ibid). Unlike Reyns and Randa (2017), Golladay (2017) found that greater amounts taken only increased reporting to credit bureaus but not financial institutions or law enforcement.\textsuperscript{18} Notably, neither study examined the effect of the time spent resolving the incident on reporting, despite evidence

\textsuperscript{17} Most demographic predictors did not significantly predict reporting in Greenberg and Beach’s (2004) model, with the exception of gender, where females were less likely to report property crimes to police than males.

\textsuperscript{18} The difference in the relationship between the amount taken and police reporting may relate to differences in coding between these two studies. Reyns and Randa (2017) logged the amount taken variable due to its skew, which will be discussed further in the Methods chapter.
that it impacts identity theft victims’ distress (Harrell 2019; Pascoe et al. 2006) and perceptions of an incident’s seriousness (Li et al. 2019).

Other situational factors were examined in both studies, with only one overlapping finding: having knowledge about the offender increased reporting to law enforcement (Golladay 2017; Reynolds and Randa 2017). The remainder of the variables included in their analyses differed significantly. For example, Reynolds and Randa (2017) found that knowledge about how one’s information was obtained increased reporting to police, while increases in the length of time one’s information was misused decreased the likelihood of reporting. They also found that contacting financial institutions increased the likelihood that victims reported to police (ibid). Golladay (2017) included measures for the number of incidents victims experienced in the last 12 months and whether they had also been a victim of identity theft before the last year. Having experienced a prior identity theft incident decreased reporting to law enforcement (ibid), which may relate to Reisig and Holtfreder’s (2007) finding that having recently been a victim of fraud decreased confidence in the police. None of the situational variables Golladay (2017) tested were significant for predicting reporting to credit card companies or banks. Finally, knowing one’s offender and having experienced additional identity theft incidents within the last 12 months increased reporting to credit bureaus (ibid).

Regarding demographics, Reynolds and Randa (2017) found that those with higher incomes were less likely to report to law enforcement. Golladay (2017) did not find a significant relationship between income and police reporting, although those identifying with a minority
race were more likely to report to both police and credit bureaus.\textsuperscript{19} With respect to financial institutions, victims with higher incomes were more likely to report than their peers (ibid). Finally, Schoepfer and Piquero (2009) examined predictors for reporting fraud victimization to police in the United States and found that those with higher educational attainment were more likely to report to law enforcement.

More recently, Gies et al. (2021) examined differences in identity theft incidents between those reported to the Identity Theft Resource Center (ITRC) compared to the 2016 NCVS – ITS sample. They found that those reporting to the ITRC had greater financial, health, and relational problems than the general ITS population, suggesting that serious incidents were also more likely to be reported to support institutions (ibid).

The advice received from others, which cannot be measured through the ITS instrument, can also inform reporting decisions. For example, Mason and Benson (1996) examined the effect of advice from others on fraud victim’s police reporting. They found that victims who were encouraged to report to police were nearly twice as likely to do so compared to those receiving no advice, while victims discouraged from reporting were three times less likely to contact police than those receiving no advice (ibid).

\textsuperscript{19} The reasons for reporting differences based on sociodemographic variables are not well understood. Reynolds and Randa (2017) observed that further research examining the role of income in reporting is worthwhile. Moreover, it is unclear why identification with a minority race increased police and credit bureau reporting in Golladay’s (2017) study. Past research has found that age and race relate to perceptions of police, with younger individuals and those identifying as non-white having less trust and lower satisfaction with police (Brown and Benedict 2002; Xie and Baumer 2019). Nonetheless, considerable variation exists within racial groups (Brown and Benedict 2002). Further research may be beneficial in examining the role of sociodemographic factors in the reporting decisions and experiences of victims of property crimes.
Moreover, reporting rates may differ between online and offline crimes, although the few studies that have examined these differences have conflicting findings. van de Weijer, Leukfeldt, and Bernasco (2019) found that Dutch victims of cybercrimes reported less frequently than those of offline crimes, whereas Kemp (2020) found that online fraud victimizations in Catalonia were reported at higher rates than offline frauds. Kemp (2020) noted that several factors that may play a role in these differences require further research, including the distance between the offender and the victim and whether self-blame occurs at different rates for online and offline fraud.

Identity theft and fraud victims can have many reasons for not reporting to police, including that they were not aware an incident occurred, that they did not perceive it as serious, that they were embarrassed, or that they reported elsewhere (Button and Cross 2017). Moreover, some fraudsters design scams that take small amounts of money from many people to decrease the likelihood that victims report to law enforcement (ibid). Harrell (2019:13) found that when American victims were asked why they did not report to police, 17 percent of victims either did not think to report to police or were not sure where to report incidents.

Some scholars have also investigated motivations for reporting. Button and Cross (2017) and Cross (2018c) outlined several needs that may motivate fraud victims’ reporting behaviours following victimization. A primary need for many victims was to recuperate monetary losses, but victims were also motivated by a desire for a formal investigation, by wanting more information or advice to prevent future incidents, or by needing emotional support (Button and Cross 2017). Cross (2018c) interviewed a sample of fraud victims who reported to the primary Australian consumer protection agency (the Australian Competition and Consumer Commission) and found that victims’ goals included having their complaint investigated, the perpetrator brought to
justice, or preventing others from being victimized.\textsuperscript{20} Finally, in the United States, Green et al. (2020b) found that victims who reported to law enforcement sometimes did so to obtain police reports to show their banks that they were victims of crime.

In summary, only two recent studies have examined identity theft police reporting, and despite using the same dataset, they included different predictor variables. While Reyns and Randa (2017) found that seriousness increased the likelihood of police reporting, studies of other victims suggest that advice and emotional reactions may also be significant for reporting decisions.

3.4.2 Victim’s Experiences with Institutions

Similar to reporting decisions, identity theft victims’ satisfaction and experiences with institutions remain understudied, particularly in North America. The research that exists, primarily from Australia and the United Kingdom, suggests that fraud reporting experiences are mixed, with many victims dissatisfied with the institutions they contact (Button et al. 2009; Cross, Richards, and Smith 2016).

Positive experiences with institutions have been reported in several studies, although they have normally preceded longer sections discussing victims’ negative experiences. Button et al. (2009) interviewed almost 800 victims of fraud in the UK and found extremely mixed experiences among participants. Some victims reported positive experiences with police and other companies: victims were often more satisfied with financial institutions when their funds were reimbursed quickly and with police when their cases were investigated (ibid). In the United

\textsuperscript{20} Unfortunately, Cross (2018c) also noted that few of these incidents were likely to be investigated.
States, Green et al. (2020b) drew from a sample of victims who reported to the not-for-profit ITRC. They found that victims had varied experiences with the institutions contacted, although several participants were satisfied with police, government agencies, and the ITRC (ibid).

Moreover, Geis et al. (2021) compared the ITRC sample to the NCVS – ITS sample and found that those who reported to the ITRC had more positive comments and fewer mental health problems than the general population of identity theft victims.

Negative experiences with institutions often result from the complexity of navigating the fraud justice network or from perceptions that institutional actors did not care to help or investigate issues. At the conclusion of Sproule and Archer’s (2008) survey of Canadian victims, they allotted space for respondents to further describe details about the fraud. While many did so, other victims used this space, unprompted, to express displeasure with institutional responses (ibid). The complaints included that victims were referred elsewhere and that they believed that financial institutions and police did not care to investigate cases (ibid).

Some fraud victims’ frustrations relate to an inability to find institutional actors that are able and willing to assist. Button et al. described a “merry-go-round” effect (2009:33), whereby some victims were repeatedly told by institutional actors to report elsewhere. Button et al. (2012) later noted that the merry-go-round effect involves both the challenge of identifying the correct institution to which to report and then finding an actor within that institution who is willing to assist. Cross (2018d) also found evidence that many victims experienced the merry-go-round effect in Australia. Moreover, some fraud victims experienced similar effects with policing agencies, where local police would refer them to federal police who may say that the case is outside of their jurisdiction (e.g., if the case is international; ibid).
The issue of victims being referred elsewhere may result from institutional actors’ unwillingness to help or from victims’ lack of knowledge of where to report. For instance, Australian scholars have found that victims may be unsure of where to report and of what institutions’ roles are in the aftermath of fraud (Cross 2018d; Cross et al. 2016). Moreover, in a sample of victims who had reported to Australian law enforcement, Cross (2020) found that many victims failed to understand the complexity of jurisdictional issues in investigating online fraud internationally and across states. Green et al. (2020b) found similar experiences in the United States, with many American victims expressing that the process of reporting and the information available to them was overwhelming.

Finally, some fraud victims’ negative experiences result from a lack of investigation or communication from institutional actors. Button et al. (2009) described victims in the UK who became frustrated by receiving little communication or advice after reporting fraud incidents. In Australia, Cross (2018d) found that when participants reported to fraud agencies and police, they were often disappointed when the information they provided was not used to launch an investigation into the fraud or its perpetrators. Other Australian victims perceived that responding institutions did not care after receiving little follow-up about investigations (Turville et al. 2010). Moreover, even when institutions followed up with victims about the nature of their incidents, many victims felt that institutions were not interested in identifying the perpetrator (ibid). Finally, Green et al. (2020b) reported that several American identity theft victims described institutions as useless.

In summary, victims report identity theft incidents to financial institutions more often than to law enforcement. Victims are more likely to contact police when incidents are more
serious, including when greater amounts are taken or when they suffer out-of-pocket loss.

Additionally, research has consistently found that fraud victims’ experiences with institutions vary. Some victims are satisfied, particularly when incidents are resolved quickly and investigated. Others have negative experiences, including when being referred elsewhere or receiving little follow-up about investigations. Finally, some victims have more unique negative experiences, such as when institutional actors are unsympathetic or provide incorrect advice (Button et al. 2009).

3.5 Summary

This chapter presented past research informing this dissertation, including processes of defining events as crimes and the self as victims as well as research on victims of identity theft and fraud. Since revisions to North American criminal codes, identity theft has continued to increase in North America. While many victims recoup losses by contacting financial institutions or other companies, non-financial consequences can include emotional distress, losses of time, and physical or relational issues.

Although few studies have examined identity theft victimization qualitatively, some research has addressed the process of realizing one has been victimized, including initial panic over potential consequences. Moreover, existing research indicates that most victims are uncertain of how the incident occurred or by whom they were victimized. Past research on victims of violence against women suggests that becoming a victim relates to one’s awareness of a crime, external definitions, typical conceptions of victims, and rationalizations. Finally, institutional messaging often encourages self-protection and places responsibility on individual consumers, and these discourses may relate to past findings that fraud victims are stigmatized.
Nonetheless, it remains unknown how identity theft victims define the incidents they experience and whether they identify as victims in the aftermath.

In terms of reporting decisions, most North American identity theft victims report to credit card companies or banks, with few contacting law enforcement or credit bureaus. The limited research investigating victims’ reporting decisions suggests that greater consequences of identity theft predict increased police reporting: when victims pay out of pocket, have greater amounts taken, or experience more distress, they are more likely to contact law enforcement. The role of other factors in identity theft reporting, such as advice and emotions, are not understood due to the lack of existing qualitative studies.

Victims’ satisfaction with the institutions they contact also remains understudied, but the research on fraud victims that exists finds mixed experiences. Some victims are satisfied with institutions when reimbursed promptly or when their case is investigated. However, many victims experience frustration, including when being referred to other institutions, when institutional actors seem uninterested in assisting, and when institutions fail to investigate or provide updates on cases. Although the most recent Canadian identity theft victimization survey found some victims experienced frustration with institutions (Sproule and Archer 2008), it remains unknown how institutions have been meeting the needs of identity theft victims since its criminalization.

The next chapter presents this dissertation’s methods. Quantitative analysis of the 2016 NCVS – ITS explores the relationships between measures of seriousness and identity theft victims’ reporting to police, financial institutions, and credit bureaus. Accordingly, it presents the most comprehensive assessment of factors influencing identity theft victims’ reporting to date.
Moreover, this research draws from active interviews with 20 victims of identity theft in Ontario to contribute qualitative insight to an area that has predominantly been studied quantitatively. These interviews provide a nuanced understanding of victims’ perceptions of the incidents and themselves along with victims’ reasonings for their reporting decisions. Further, they allow for the investigation of identity theft victims’ experiences with reporting and their satisfaction with the resolutions: areas that have to date been neglected in Canadian research.
4 Methods

4.1 Introduction

To investigate the experiences and decision-making of identity theft victims, this study drew from active interviews with 20 victims of identity theft in Southern Ontario and quantitative analysis of the 2016 United States’ National Crime Victimization Survey (NCVS) – Identity Theft Supplement (ITS). The research questions guiding this study were:

1. a) How do those who have experienced identity theft understand the incidents – be it as crimes, inconvenient events, or otherwise?
   b) Do those who experience identity theft victimization identify themselves as victims of crime?
2. a) Do those who have experienced identity theft formally report it? If so, to whom?
   b) Why do those who have experienced identity theft choose to report or not report to specific institutions (e.g. police, credit card company, etc.)?
3. How satisfied are victims with the resolution facilitated by the institutions they approach?

Pragmatic methodologists suggest using the tools available that are most appropriate for examining the research questions (Johnson and Onwuegbuzie 2004). Grounded in interactionism, this study involved an interactive mixed methods design to address its research questions and draws from both interview and survey data. Specifically, interview data allowed for examination of the first research question, concerning victims’ understandings of their victimizations and selves, and the third research question regarding victims’ satisfaction with the institutions contacted. Further, both interview and survey data were used to investigate the second research question concerning victims’ reporting decisions.

This chapter begins by discussing the mixed methods design of the study. Following this is a discussion of the quantitative data, sample selection, and analysis procedures. Finally, this chapter describes the interview recruitment, approach, and process as well as the methods of qualitative analysis.
4.2 Mixed Methods Approach

Mixed methods research can be beneficial for assessing trends in actions while simultaneously investigating individuals’ experiences of a phenomenon (Creswell 2015; Creswell and Plano Clark 2018). This study used an interactive mixed methods design, incorporating findings from both qualitative and quantitative analyses to examine reporting decisions following identity theft victimization (Research Question #2). An interactive approach to research design is flexible and emphasizes that choices about a study’s goals, theoretical framework, research questions, methods, and assessment of validity can inform one another multi-directionally (Maxwell 2013; Maxwell et al. 2015; Maxwell and Loomis 2003). Maxwell (2013) positioned interactive approaches to mixed methods in contrast to typological approaches, which are more structured and guided by a typology that is often selected at an early stage of the project (see Creswell 2015; Creswell and Plano Clark 2018). While an interactive approach involves choosing the methods best suited to address the study’s research questions, it also requires an understanding of the research design as a process, which can involve adjustments based on challenges faced. Further, Maxwell (2013) emphasized the situated nature of researchers and argued that there is a tendency for scholars to present design choices as separate from researchers’ experiences and resources, which neglects important factors in decision-making.

21 Additionally, brief surveys were administered to interview participants and were used in the analysis of interviews, described below. Thus, Research Question 1 and 3 were answered primarily by drawing from interview data, but interview participants’ survey responses also informed these questions. While I propose that Research Question 2 is the only one that is explicitly informed by both analyses, a broader interpretation of mixed methods research may understand the interviews’ analysis procedure as a mixed methods undertaking (see Maxwell 2016 for a discussion of the range of studies that could be defined as mixed methods but are not labeled as such).
In this study, a significant research design choice was to use qualitative and quantitative data from different social contexts. While there are some differences in the legal definitions and institutional responsibilities surrounding identity theft in the United States and Canada, there is considerable similarity. The research questions aimed to identify patterns in actions taken by victims and to understand their experiences in-depth, thus making survey analysis and interviews beneficial. I made use of the NCVS – ITS due to the lack of existing comparable Canadian data and the costs required to conduct a large-scale survey. The United States’ NCVS – ITS is unmatched in terms of the scale and depth of insight it provides on identity theft victims. Further, I conducted interviews in Southern Ontario for convenience and due to its high population density.

Overall, the goal of combining methods was to gain a more complete understanding of victim reporting decisions. Given that the NCVS – ITS has been a primary source of knowledge on identity theft victimization in North America since its creation in 2008, its survey instrument informed some of the questions posed to interview participants. Nonetheless, unlike a sequential explanatory design where quantitative analyses precede qualitative analyses (Creswell 2015), interview and survey data were initially examined independently prior to their comparison. Thus, the present study embraced the capacity for mixed methods to provide complementary but divergent insights (see Greene 2007; Maxwell 2013; Maxwell and Loomis 2003) rather than triangulating findings. In some cases, interviews provided insight into trends identified in

---

22 For example, the Canadian Government recommends victims report identity theft to both local police and the Canadian Anti-Fraud Centre, which collects information on identity fraud and theft (Canadian Anti-Fraud Centre 2021), while the United States Department of Justice (2021) recommends American victims first report identity theft to the Federal Trade Commission.
quantitative analyses. An example is the influence of out-of-pocket losses on reporting decisions: quantitative findings indicated that suffering out-of-pocket losses was a predictor of police reporting and several interview participants who did not report to law enforcement cited their lack of out-of-pocket loss as a reason. Therefore, this study’s design was based on a pragmatic interactive mixed methods approach, where the methods were chosen based on the data best suited to address the study’s research questions.

4.3 Quantitative Methods

This study’s second research question concerned whether and to whom victims choose to report identity theft incidents. As such, this study drew on quantitative analyses of the 2016 United States’ NCVS – ITS to provide insight into trends in the reporting decisions of identity theft victims. Interactionism is commonly associated with qualitative inquiry with close proximity to the social world in order to study actions and meaning. However, some schools of symbolic interactionism have used statistical methods to quantify interactionist concepts such as self-attitudes (Couch 1958; Kuhn and McPartland 1954) and affect (Heise 1977). Moreover, it is increasingly recognized within interactionism that quantitative methods are beneficial for certain studies (Fine 1993; Maines 2003), in part due to their capacity to summarize trends in social actions (Ulmer and Wilson 2003). As such, I performed quantitative analyses to identify situational factors influencing decisions to report identity theft victimization to law enforcement, financial institutions, and credit bureaus.

4.3.1 Data

The NCVS collects data about criminal victimization from a nationally representative sample of American households. In addition to collecting information about the prevalence of
victimization, victims are asked about the incident’s circumstances and their reporting decisions. Interviews are conducted in person and over the phone every six months for up to three and a half years. The Identity Theft Supplement (ITS) was first created in 2008 and is administered every two years to individuals aged 16 years and older within the households included in the NCVS sample.23 The overall response rate of the 2016 NCVS – ITS was approximately 61 percent. Nonetheless, Harrell (2019: 17) conducted a non-response bias analysis and found little to no bias with the ITS data. All data were weighted to account for the sampling design.

This study included all respondents who answered “Yes” to at least one of the screening questions indicating that they had been victim to identity theft in the prior 12 months. The screening questions for identity theft victimization included whether the participant had experienced the misuse of an existing credit card, bank, or other account; the creation of a new account in their name; or the misuse of personal information for any other fraudulent purpose. Further, due to variable selection, only those victims who had some value of money, goods, or services taken were included in the analysis; these inclusion criteria are similar to Reyns and Randa’s (2017) study of identity theft victim reporting, as several key independent variables, including suffering out-of-pocket loss and the time spent resolving the incident, were only asked to those who had some money taken. Approximately one third of the NCVS – ITS sample had nothing of value taken and were excluded from the analyses. Further, just over 10 percent of victims had not yet resolved issues related to the incident and were excluded from analyses since the length of time the incident took to resolve was included as a measure of seriousness. In total,

23 The 2018 NCVS – ITS was released after I had written the methods and completed the quantitative analyses, but before completion of the dissertation.
nearly 60 percent of identity theft victims in the 2016 NCVS – ITS sample were included in the analyses.

4.3.2 Variables

The three dependent variables were whether the victim reported to law enforcement, financial institutions, and credit bureaus. These institutions are the most common ones to which victims report identity theft according to the 2016 NCVS – ITS data and previous iterations (see Golladay 2017). All three variables were coded such that 0 = No and 1 = Yes based on questions asking whether the respondent contacted the specified institutions (see Appendix A for the full list of variable coding). Law enforcement includes local police, sheriffs, and federal law enforcement while financial institutions include banks and credit card companies (see Appendix B for the full list of questions).

Reyns and Randa (2017) noted that empirical research has not examined what factors relate to perceived seriousness for identity theft victimization. Nonetheless, their study of reporting decisions identified likely measures of seriousness that are analogous to other crimes, including the amount taken by the perpetrator, whether the victim suffers out-of-pocket losses, and emotional distress (ibid). Therefore, these measures of seriousness were included as independent variables. The variable for the amount taken from the victim prior to recuperation was positively skewed. As such, similar to Reyns and Randa (2017), the amount taken variable was logged as a precaution to account for the potential effect of outliers. Suffering out-of-pocket personal financial loss was coded such that 0 = No and 1 = Yes, and distress was measured on a Likert-type scale ranging from 1 = Not at all Distressing to 4 = Severely Distressing. The present study also included time spent resolving the incident as a measure of seriousness, since it is a
significant cost of identity theft victimization (Copes et al. 2010; Harrell 2019) that can force disruptions in daily life, including missed work and cancelled plans (Identity Theft Resource Centre 2018). Time spent resolving the incident was measured on a seven-point scale ranging from 1 = One Day or Less to 7 = One Year or More.

Other situational factors that may influence reporting decisions were also included as independent variables. Research in the United States finds that experiencing a prior identity theft incident decreases the likelihood of reporting to police (Golladay 2017). Additionally, knowledge about the offender is theorized to influence reporting decisions (see Gottfredson and Gottfredson 1988) while knowledge of how one’s personal information was obtained could influence perceptions about whether police could realistically respond (Reyns and Randa 2017). As such, having previously experienced identity theft, having knowledge about the offender, and knowing how one’s personal information was obtained were coded such that 0 = No and 1 = Yes. Reyns and Randa (2017) found that the longer one’s personal information is misused, the less likely they are to report to police; they hypothesized that the length of time one’s information was misused may influence their perception of urgency in resolving the incident. The length of the misuse prior to its discovery was coded on a seven-point scale ranging from 1 = One Day or Less to 7 = One Year or More. Finally, when notified by a financial institution, victims’ reporting decisions are likely influenced by the actions they are advised to take, and this variable was coded dichotomously (0 = No and 1 = Yes).

Demographic variables that may influence reporting decisions and attitudes about police and institutions were included as control variables. Age was measured in years (range = 16 to 90), while annual household income was coded into 14 categories, from 1 = Less than $5,000 to
14 = $75,000 and over.\textsuperscript{24} Education was coded into five categories from 1 = Less than High School to 5 = Advanced Degree. Gender (1 = Female) and marital status (1 = Married) were also included as dichotomous control variables. A measure of race/ethnicity is the product of combining race and Hispanic origin variables to create four categories: White, Black, Hispanic/latinx, and Other.\textsuperscript{25} Finally, region of the United States was divided into the Northeast, Midwest, South, and West.

4.3.3 Method of Analysis

Data were analyzed using logistic regression since each dependent variable is dichotomous. Logistic regression can produce odds ratios, which describe the effect of each independent and control variable on the dependent variable. Simply, odds ratios refer to one’s odds of reporting with a one unit increase in that variable over the base odds of reporting. For example, for the variable measuring respondents’ gender, the odds ratio represents the odds of reporting for females over the odds of reporting for males. An odds ratio greater than one would imply females have a higher likelihood of reporting than males while an odds ratio less than one would imply males have a higher likelihood of reporting than females.

For each of the three dependent variables, eight models were estimated. Model 1 examined the effects of the four measures of seriousness on the victim’s likelihood of reporting identity theft to law enforcement, a financial institution, or a credit bureau. Model 2 examined the effects of other situational variables, including experiencing a prior identity theft incident.

\textsuperscript{24} Income was coded in line with the Inter-University Consortium for Political and Social Research’s (ICPSR) release of the 2016 NCVS – ITS. In cases where respondents did not know or disclose a household income, it is drawn from the household representative interviewed for the NCVS.

\textsuperscript{25} Following Harrell (2019), the categories White, Black, and Other exclude those individuals who identify as Hispanic/latinx.
knowing about the offender, knowing how one’s personal information was obtained, the length of time the information was misused, and the two other reporting options. For instance, in the models examining police reporting, reporting to credit bureaus and financial institutions were included as control variables. Model 3 included both measures of seriousness and situational variables while Model 4 examined the effects of demographic variables on reporting. Model 5 is the full model and included all independent and control variables.

Koops and Leenes (2006) observed that in many cases of identity theft, individuals’ identities can be conceptualized as tools for victimizing institutions rather than as the target of the crime. Consequently, those who suffer out-of-pocket losses may be more likely to see themselves as the target of the crime, which could influence their reporting decisions. Accordingly, and tied to the first research question, Models 6 through 8 tested interaction effects to determine whether predictors impacted reporting decisions differently based on whether victims suffered out-of-pocket losses. Specifically, these models explored interactions between suffering out-of-pocket losses and distress, amount taken, and time spent resolving the incident, respectively.

Few variables had missing data and, of those identity theft victims who had some value of goods or services taken and had resolved the incident, only two variables had over 0.5 percent of values missing: the length of time one’s identity was misused (3 percent) and age (2 percent). Listwise deletion was therefore appropriate for handling the missing data as the probability of having missing cases on these independent variables was unlikely to be influenced by one’s
response on the dependent variables\textsuperscript{26} (see Allison 2002). The final analytical sample included 5,753 participants, which was sufficiently large to permit statistical inferences.

4.4 Qualitative Methods

4.4.1 Recruitment

To investigate how victims understand identity theft incidents, I conducted in-depth interviews between August 2019 and September 2020. My goal was to access participants with diverse backgrounds and experiences with identity theft incidents. Participants were recruited using convenience sampling through posters placed at family and financial counselling centres, posts on Reddit (www.reddit.com), and a post on the University of Guelph’s Office of Research website.

Recruitment posters (see Appendix C) were displayed at two family and financial counselling centres in Southern Ontario. I approached managers at these organizations as they were part of a network of not-for-profit counselling centres with interests in financial literacy and education that align with this study’s interests. In correspondence, the managers described that their clientele are diverse members of the community attending for various counselling needs, which fits with the goal of accessing participants with a range of backgrounds and experiences.

Additional participants were recruited online through Reddit. The self-proclaimed “front page of the internet,” Reddit is a social media and discussion website that allows users to post external or text-based content on which other members vote to determine the order in which

\textsuperscript{26} An additional concern with listwise deletion is that it leads to reduced cases which can impact statistical power (see Cheema 2014). However, with this sample’s small proportion of missing cases and large sample size, the loss of statistical power is expected to be minimal.
posts appear. Reddit is divided into communities, called “subreddits,” that are organized around particular topics, social groups, regions, or types of content. I submitted recruitment posts to approximately 30 community subreddits across Southern Ontario. Although Reddit allows attachments, the posts were made as text-based submissions with details about the study, eligibility criteria, and contact information. I first submitted posts to the subreddits for the two communities where counselling centres had flyers posted, then to subreddits for other communities in Southern Ontario. Finally, I posted advertisements on a subreddit dedicated to recruitment for academic and non-academic research. I primarily submitted posts on weekday mornings to ensure that they were visible throughout the afternoon and evening and to allow for potential participants to receive timely responses to inquiries. I made a maximum of two posts per week to ensure participants would receive quick replies and to show regular engagement with communities. Participants were offered a $20 gift card for gas, groceries, or Amazon.ca as an incentive for participating.

As the first research question related to victims’ understandings of the events before them, legal definitions including the terms “victim” and “identity theft” were omitted from recruitment materials. This was inspired by Emerson, Ferris, and Gardner’s (1998) study of

27 I followed subreddit rules and etiquette to gain support from moderators. In one subreddit, the recruitment post was submitted as a reply in an advertisement thread. In other communities, recruitment posts were not permitted. Finally, subreddit moderators removed four posts despite them adhering to subreddit rules.

28 Because of Reddit’s voting system and the fact that posts lose visibility over time, it is not possible to determine for how long each individual post could be regularly seen. The visibility of a post depends on the number of positive votes it receives, the time since its submission, and its popularity and time of submission relative to other posts made on that subreddit. Technically, if users wanted to scroll through pages of content on these community subreddits, these posts could be visible indefinitely.

29 On Reddit, the posts and activity of a user can be viewed by other users. As such, I maintained positive activity and posted sparingly to avoid being viewed negatively as a ‘spammer.’
stalking victims. They understood stalking as a process and avoided the use of the term in recruitment in order to include those who may not have defined themselves as victims or the events as stalking. Similarly, Goffman’s (1974) *Frame Analysis* began with the assumption that individuals routinely ask, “what is it that’s going on here?” when confronted with situations (p. 8). Therefore, this study was framed more generally as an investigation of the misuse of accounts or personal information. Avoiding the terms “identity theft” and “victim” in recruitment materials allowed for the enlisting of participants who viewed the incident through frames different from those of the researcher.

Overall, 20 individuals participated in the study, most of whom found out about the study through Reddit. When asked, some participants were unsure whether they saw the post on Reddit or elsewhere online, and multiple participants were forwarded the study information by someone close to them who saw a recruitment post. Initial interviews were conducted in person in a private office, with an option for telephone interviews for those unable to coordinate a meeting. Prior to the COVID-19 pandemic, four interviews were conducted in person and three were conducted over the telephone to facilitate participants’ work and family schedules. As concern grew about the COVID-19 pandemic and the University of Guelph halted in-person research, all remaining interviews were conducted over the telephone. While telephone communication negates the ability for non-verbal communication and cues, Holt (2010) noted that the medium can encourage greater detail during narrative responses.

Overall, the interview participants were younger than the NCVS – ITS survey respondents: 85 percent of interview participants were between the ages of 18 and 40, which broadly reflects the demographic of Reddit users (see Shatz 2017). Twelve males and eight
females participated in the study. The most common occupations that participants described were information technology, marketing, and university student. In terms of reporting decisions, 10 percent of interview participants contacted police compared to 5.9 percent in the survey sample, and 15 percent of interview participants contacted credit bureaus compared to 5.8 percent in the survey sample.\textsuperscript{30} Fewer interview participants (65 percent) reported to financial institutions than respondents in the NCVS – ITS sample (94.6 percent), which may be a product of the inclusion criteria for the quantitative analyses. Further, more interview participants (15 percent) than survey respondents (5.8 percent) knew their offender. The interview participants who knew their offender did not report to law enforcement or credit bureaus and only one reported to a financial institution. Based on interviews, their overrepresentation in the qualitative sample may have resulted from a desire to talk to someone about their experiences in a confidential setting.

\textbf{4.4.2 Surveys}

After an informal conversation aimed at building rapport, participants completed a brief survey about the most recent incident of identity theft they had experienced (see Appendix D). The survey was mostly comprised of closed-ended questions from the NCVS – ITS related to their reporting decisions and consequences of the incident. Questions asked whether participants reported to financial institutions, credit bureaus, and law enforcement, and, if applicable, inquired about their satisfaction with these institutions. For those who did not report to law enforcement, the survey asked why they chose not to report. Finally, questions were asked about the amount taken, the amount of out-of-pocket loss, the time spent resolving the incident, the

\textsuperscript{30} Full descriptive statistics for the quantitative variables are described in Chapter 6.
amount of distress experienced, and whether they had an idea of how the incident occurred. Some questions were modified slightly from the NCVS – ITS questionnaire to better fit the Canadian context. These surveys were used to compare the interview sample with the respondents from the 2016 NCVS – ITS. Further, these questions allowed for the comparison of interview data based on differences in survey responses.

4.4.3 Interviews

I conducted semi-structured active interviews about participants’ experiences with identity theft, the consequences they faced, and their reporting decisions following the incident. With participants’ consent, interviews were audio-recorded and transcribed in full. The open-ended interview component lasted from 22 minutes to 66 minutes ($M = 39$ minutes). Active interviewing allows the researcher to understand the substantive incidents and actions taken while also attending to how participants think about, understand, and construct their experiences (Holstein and Gubrium 1995). From an interactionist perspective, participants’ responses are not mere reproductions of events being recounted; rather, they are influenced and informed by the questions posed, the relationship formed, the social dynamics of the interview, and the participants’ expectations and goals upon entering the interview.

Active interviewing represents an “orientation to the interview process” (Holstein and Gubrium 2004: 6) rather than a procedure for interviewing. Contrary to the view that interviewers should avoid influencing participants’ responses, active interviewers understand and embrace the fact that meaning is interactionally constructed during interviews (Holstein and Gubrium 2004: 6).
The active interviewer attempts to gain insight into participants’ assumptions by provoking responses that make use of a variety of the participants’ interpretive resources (ibid). Techniques implemented by active interviewers range from “playing dumb” (Becker 1954: 32) to more direct challenges of participants’ responses (see Hathaway and Atkinson 2003). Further, participants often use aspects of interviewers’ social identities, including ethnicity, gender, and occupation, to position the interviewer in terms of commonalities or differences (Song and Parker 1996). Interviewers may work to balance their position as both insider and outsider to elicit deeper understandings of participants’ assumptions, though the success of such strategies depends on the participants’ perceptions of the interviewer (Abell et al. 2006; Hathaway, Sommers, and Mostaghim 2020).

Interviews began with a narrative component asking the participant to describe the story of a time their identity information or account was misused without their consent. Narrative interviewing can be beneficial for understanding the incident in the participants’ own terms without imposition by the interviewer (Scheibelhofer 2008). Further, narratives can present participants’ assumptions regarding the substantive topic, which may reflect group norms (Wengraf 2001). From an interactionist perspective, narrative storytelling presents a form of human activity that recounts actions and experiences and often presents these in the terms of common social conceptions (Maines 2001). The goal of the narrative phase was to understand the events and actions that participants perceived as important to their experiences of identity theft. Accordingly, the participants’ conceptions of the incident and themselves sometimes became evident during this phase. The narratives that participants present during interviews are distinct storytelling constructions that are, in part, informed by the interactional dynamics of the
research interview (Gubrium and Holstein 1998). For instance, narratives can be influenced by the recruitment process and materials or by rapport-building. Following one participant’s narrative, they paused, then said: “Yeah, I don’t know if that’s good or what else you need…” This illustrates that participants may emphasize aspects of their story that they expect will be of interest to the researcher.

The next phase of interviews included open-ended questions and discussion about the identity theft incident. An interview guide was created prior to the interviews, but questions were not exhaustive and were instead used to guide the conversation when necessary (see Appendix E). Follow-up questions often evolved naturally from the narrative and provided a beneficial transition into the more conversational open-ended discussion (see Scheibelhofer 2008). Further, I asked questions related to the research questions when they were not addressed in the participants’ narratives. For example, where participants omitted details about whom they contacted after the incident, I asked to whom they reported and why. Questions were also asked regarding interactions with friends and family following victimization and about the participants’ relationships to the offenders. Near the end of this phase, I asked participants what they would recommend to someone who found themselves in a similar position. The goal of this question was, in part, to understand participants’ experiences with and expectations of the institutions involved.

Throughout the interview, I reflexively asked questions to better ascertain participants’ assumptions and the social resources from which they drew. In some instances, my status as a researcher of identity theft made playing dumb seem unfeasible, and I more directly challenged participants’ responses. For example, when a participant discussed the inevitability of identity
theft, I asked if it is something we must accept. One participant, who was victimized by a company’s employee, took the perspective of such an employee and speculated that the risk for incidents is high because many employees may be tempted to misuse information from customer databases. When asked whether this was something the customer must accept, the participant expressed:

I feel like we should never accept it, because that kind of makes it seem like it’s okay for a second, but I feel like we should always just be aware that there’s a possibility it might happen… but also knowing as well, that there are serious consequences behind stuff like this, that the odds of the person actually getting away are very slim but it’s still a headache [laughs] to have to go through it and everything. So yeah, I don’t think we should accept it.

After challenging the participant with the perspective of the customer, their line of response shifted away from the perspective of the employee, thus describing how identity theft is not “okay.” This response illustrates several themes that will be discussed further in Chapter 5, including the inconvenience of these events and institutions’ roles in victimization.

In other cases, it was possible to assume the outsider role by asking for further information or what the participant meant by common phrases. For example, I could sometimes embrace the role of someone who had not experienced identity theft victimization, which allowed me to ask for further details when participants discussed emotions related to the incidents. In one interview, I asked the participant what they would recommend to somebody who had just found out their account had been misused. In response, the participant eventually said:

Participant: “…so yeah, I would just say uh, kind of put your ego aside and just look for a resolution as quick as possible and be as proactive as possible.”

Interviewer: “Can I just dive in… what do you mean ‘put your ego aside’?”

89
Participant: “Oh, I mean, for me, I was like, ‘Oh, I don’t want to think like I’m an idiot’ kind of thing. Like, I don’t want to be embarrassed, that sort of thing. So, just don’t be like afraid to look like a fool kind of, for a second...because at the end the day, you might think ‘Oh I’m really stupid for having this happen to me’, and like, I’m sure the bank isn’t going to be like, or whoever you contact isn’t going to be like: ‘Oh, you’re an idiot, why did you do that?’, they are just going to be like: ‘Yeah, we’ll help you.’ So like, you need to put your ego aside and not be afraid to be vulnerable kind of thing.”

Asking for elaboration on this common phrase led to the participant further describing their hesitancy to seek assistance based on the anticipated reactions of others. Similarly, assuming the outsider role allowed me to more directly question participants’ assumptions about identity theft victims. For example, when I asked one participant how they would like to be described, the exchange went as follows:

Participant: “I suppose if you describe me as a software developer, it might give weight to the fact that I wasn't being like haphazard online and stuff like that. You know, that I have some understanding of technology.”

Interviewer: “Now we're going to have to dig into this statement, is there some sort of assumption here that the people this happens to are in some way not tech-savvy?”

Participant: “I mean, yeah. I think that perception does exist. You would say, ‘Oh it's happening to, like old grandmothers.’”

By probing participants about their assumptions, their conceptions of typical victims of identity theft became apparent, which will be discussed further in the following chapter. In sum, the active interviewing approach allowed for an understanding of the situated nature of responses and deeper questioning based on interactional dynamics during the interview.

4.4.4 Coding

I analyzed interview data in multiple coding stages similar to the process of grounded theory coding described by Charmaz (2014) and inspired by the constant comparative method proposed by Glaser and Strauss (1967). Grounded theory methods are flexible procedures for
conducting research with the goal of producing theory from the data (Charmaz 2014). The techniques outlined in grounded theory coding align with interactionism through their focus on coding for actions, their emphasis on analysis as process, and their attention to emergent themes. Although stages are demarcated within grounded theory coding, they are non-linear since analyses in the form of comparison to existing codes occur throughout the process. Initial coding involves reviewing transcripts line-by-line and creating codes that attend to actions. By focusing on actions described by participants, grounded theory coding strives to ensure that the themes identified closely reflect the data without applying more abstract concepts at an early stage (ibid). Focused coding involves the identification of codes that synthesize and reflect the initial codes that arise numerous times across interviews (ibid).

I used NVivo 12 to facilitate the organization of codes. The coding process was iterative and involved revisiting prior codes, transcripts, and texts. During the interviews and their subsequent transcription and re-reading, I recorded memos when trends and themes emerged. I performed line-by-line coding on all interviews to ensure that the themes identified were not restricted based on prior conceptions. Beginning during the line-by-line process, I compared similar codes to start identifying themes. After line-by-line coding was complete, focused coding involved revisiting and comparing codes that had either arisen multiple times or presented opposing actions or sentiments by participants. I organized codes based on their relationships to one another and their connections to the research questions.

In addition, the analysis involved comparisons of themes and responses within and across groups of participants. I used the survey responses to compare qualitative codes from participants who differed on key variables. These variables included whether the participant suffered out-of-
pocket losses and whether the participant knew how their information was obtained. For example, I analyzed differences in participants’ self-perceptions based on whether they suffered out-of-pocket losses. Further, comparisons in qualitative responses were examined across gender and age categories.

4.5 Summary

In summary, the present study’s research methods and analyses were guided by an interactionist and pragmatic approach. This study drew from the NCVS – ITS to examine trends in factors influencing reporting decisions of victims. Further, quantitative analyses allowed for an examination of whether suffering out-of-pocket losses as a result of identity theft had a moderating effect on the relationship between other consequences and reporting. Qualitative data contributed to knowledge about victims’ perceptions of identity theft incidents, their reporting decisions, and their experiences with the various institutions to which they reported. The active interviewing approach provided the opportunity to understand participants’ assumptions about identity theft and the institutions responsible for its resolution. By attending to meaning, this approach also enabled an understanding of how participants conceptualized identity theft victims and how they compared their experiences to these conceptions. In turn, this study was able to examine how the way victims understand the incident and their selves relates to reporting decisions and outcomes. The next chapter will examine participants’ understandings of identity theft and themselves in the context of the incidents they experienced. Subsequently, Chapter 6 will examine victims’ reporting decisions following victimization and their satisfaction with the institutions contacted.
5 Results 1: Victims’ Understandings of Identity Theft and Self

5.1 Introduction

Based on interviews with victims of identity theft, this chapter addresses the first research question by reporting findings on victims’ conceptions of identity theft and of themselves in the context of these incidents. In this chapter, I argue that victims’ understandings of identity theft incidents and themselves are processes. Further, identity theft is not simply defined as either criminal or normal; instead, participants use definitional terms associated with multiple “frameworks of understanding” (Goffman 1964:10) when conceptualizing incidents. Based, in part, on the nature of the incident and the victims’ knowledge about how it occurred, victims frame incidents in multiple ways, including as criminal incidents, inevitable inconveniences of modern life, institutional security failures, and relational issues. Even following victimizations where costs to the victims are relatively high, victims may not define the events as criminal.

Further, I argue that participants’ acceptance or resistance to victim labels depends on multiple factors. First, self-definitions relate to the social framework(s) within which the individual conceptualizes the incident. Second, participants may resist victim labels and rationalize incidents for multiple reasons, including by denying victimization occurred through self-blame or by denying harm was done by comparing oneself to other victims who suffer greater costs. Finally, some individuals hold prior conceptions of identity theft victims as naïve, old, or non-technologically savvy, which, when compared to one’s own experience, can inform self-definitions.

In what follows, I report on identity theft victims’ conceptions of the events experienced and themselves in the context of the incidents. This chapter first describes the forms of incidents
that participants experienced, then discusses participants’ common conceptualizations of these incidents. Following these summaries, I argue that defining incidents is a process which can be impacted by external definitions, the amount of information available about the incident, and comparisons to other crimes. Finally, I discuss participants’ self-identifications following identity theft and their acceptance and resistance to the victim label, which often involved comparing one’s experience to other victims.

5.2 The Events Experienced

Interview participants faced a range of forms of identity theft victimizations. As summarized in Table 5-1, eleven participants were victim to the misuse of an existing credit card, four to the misuse of an existing bank account, and nine to the misuse of another existing account, including telephone, online payment, and retail accounts. Two participants were victim to new account openings in their name, while two others were victim to other fraudulent misuses of their personal information. These totals include those participants who described multiple victimizations. Further, some incidents involved multiple forms of identity theft by the same perpetrator within a short amount of time. For example, Benjamin\(^{32}\) experienced the misuse of both an existing credit card and a bank account by a loved one.

<table>
<thead>
<tr>
<th>Form of Identity Theft</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misuse of Existing Credit Card</td>
<td>11</td>
</tr>
<tr>
<td>Misuse of Existing Bank Account</td>
<td>4</td>
</tr>
<tr>
<td>Misuse of Existing Other Account</td>
<td>9</td>
</tr>
<tr>
<td>Creation of New Account</td>
<td>2</td>
</tr>
<tr>
<td>Other Fraudulent Misuse of Personal Info</td>
<td>2</td>
</tr>
</tbody>
</table>

\(^{32}\) All names are pseudonyms.
The consequences of the incidents varied considerably across participants. Four participants had no money, goods, or credit taken, while five had over $1,000 taken. Three participants knew their offender, all of whom were victim to the misuse of their bank account by a parent and reported relational strains. Two participants suffered out-of-pocket losses, including one who was victim to existing account fraud and a second who was the victim of new account fraud. The time that participants spent resolving the incident varied, from less than a day to experiencing ongoing issues years after the initial incident. Emotional reactions to victimization were common and included anxiety, stress, anger, feelings of vulnerability, and embarrassment. Finally, some participants faced unique consequences, such as missing work, losing a job opportunity, and taking a leave from an education program.

5.3 Defining Identity Theft Incidents

The present study finds that victims understand identity theft to exist at the intersections of several social dimensions. Some participants framed identity theft incidents in multiple ways or changed their conceptualization of incidents over time. Most victims understood the incident as a crime at some point, although some downplayed the incident in comparison to other crimes, framing it as “technically” a crime (or using similar terms). Several participants defined the incidents as minor inconveniences, and relatedly, many participants discussed the inevitability of breached accounts and compromised information. Others framed victimizations as breaches of institutions’ procedures or security or theorized that the incidents resulted from clerical errors or mistakes made by institutions. Finally, the three individuals who were victimized by family members understood the incidents primarily as relational issues.
Interestingly, the type of identity theft experienced did not determine how participants conceptualized the incident. Of the forms of identity theft, only existing bank fraud was disproportionately associated with a particular definition: three out of the four participants who experienced bank fraud were victimized by a family member and thus defined the incident, at least in part, in relational terms. Definitions of the incidents varied for the remaining forms of identity theft. Some participants who experienced existing credit card and other account fraud described the incident as a crime while others did not. Of those whose information was misused for another fraudulent purpose, Sydney framed the incident in criminal terms, while Winston initially did, then came to view the incident as a clerical error. In the cases of new account fraud, Dalton was confident that it was a crime, while Courtney said that she had not previously thought of the incident in criminal terms. In this comparison, the former paid out-of-pocket loss where the latter did not. However, of the victims suffering out-of-pocket losses, Dalton described the incident in criminal terms where Benjamin understood it as a relational issue. I will describe each of these framings further, then argue that conceptualizing identity theft incidents is a process, with definitions informed by the amount of knowledge the victim has about the nature of the incident, their interactions with institutional actors, and their comparisons to other crimes and cultural depictions of identity theft.

5.3.1 As Crime

Many participants understood the incidents as crimes. When I asked whether participants saw the events as crimes, they often answered affirmatively, and some defined the incident in criminal terms without prompting, including using the terms “identity theft” and “fraud.” Dalton is a small business owner who was denied for a loan and later discovered that a line of credit had
been opened in his name, ultimately costing him several thousand dollars out of pocket. Dalton saw this as a crime: he reported the incident to police, used the term “fraud” throughout the interview and, when asked if the incident was a crime, simply replied: “Yeah. That was a crime.”

Other participants were also direct and quick to answer positively when asked if the incident was a crime. Edward is a salesperson and experienced multiple identity theft victimizations. The most recent incident occurred when he was beta-testing a software program and had his computer compromised, allowing a hacker to gain access to his Amazon account. Although most identity theft victims have little information about their perpetrator, Edward was able to see the address where products were shipped and he expressed anger toward the perpetrator. When asked if this was a crime, Edward replied: “Yes.”

Sydney is a university student whose information was misused by a healthcare employee to fraudulently access health supplies. Prior to asking if she saw the incident as a crime, Sydney used criminal terms to compare the incident to credit card fraud her mother experienced: “my mom had identity theft happen to her and stuff as well.” When asked whether she saw the events as a crime, Sydney replied yes, and expanded: “I feel like it’s something that was stolen… I feel like it was, like, identity theft, which is illegal, and then also, like stealing something from somebody else.”

Legal definitions, including the terms “identity theft” and “identity fraud,” were not included in recruitment materials or in the participant survey. Nonetheless, like in the cases of Dalton and Sydney, several participants used the terms unprompted in their narratives or at other times during the interview. Nolan is a university student and athlete who had his physical credit card stolen and misused at a bar. When asked about “these problems” generally, Nolan said:
I think, like, identity theft and that sort of thing seems so far away and so crazy to like wrap your head around. But at the end of the day, what happened to me is like, a type of identity theft.

Similarly, Regan was running a small business at the time of the interview and experienced the misuse of her PayPal account as well as an attempt to illegally port her phone account. At one point, Regan said: “…but, I mean like, no one wants to have their phone stolen or their identity stolen or anything, right? Like that's kind of a crappy thing to happen.” These examples of participants bringing up legal terms unprompted illustrate that many victims understand these incidents as crimes.

Finally, few participants denied that the incident was a crime when asked directly. Those who did include Benjamin, who was victimized by a family member and framed it in relational terms; Amanda, who framed the takeover and misuse of her social media account as trolling; and Winston, who initially thought of the incident as a crime but came to understand it as a clerical error. All three will be discussed further below.

5.3.1.1 Technically

When participants were asked whether they saw the incident as a crime, another common response was to say it was “technically” a crime. Victims who framed the incident in this way often rationalized the events as minor and sometimes compared their experience to more serious incidents. This ties to how conceptualizing incidents is a process, which will be discussed further in the subsequent section.

33 Some interviews were conducted during the COVID-19 pandemic, with public health measures resulting in the closure of some businesses. In the case of Regan, she had been employed in other professions prior to the pandemic but identified as an entrepreneur at the time of the interview. Some participants interviewed during the pandemic were not forthcoming with their employment statuses, which may reflect layoffs and employment uncertainty during the pandemic.
Kathryn is a young parent who worked part-time at the time of the interview while taking care of her child. She received a call from her bank inquiring about a suspicious transaction on her credit card, which Kathryn noticed and identified as credit card fraud. When asked whether she considered herself a victim of a crime, Kathryn replied: “Um, I mean, I probably wouldn’t use those terms myself, because I feel like [laughs] comparatively, there’s so much, you know, like worse, problems of crime…but I guess, technically, yes.”

Even some of those who used criminal terms unprompted in their narratives, like Regan, shared this perspective:

Interviewer: Do you consider yourself a victim of a crime? Or did you at the time?

Regan: I do and I don't, if that make sense.

Interviewer: Yeah, if you can elaborate that’d be fantastic.

Regan: Like, yes, it was an attempted theft, but it wasn't anything I couldn't handle. Like because I have such high faith in our-, I guess the accounts that I use, I knew that it wouldn't be a big deal.

From these examples, it is apparent that some victims acknowledge that the incident fits within criminal terms but view the incident as less serious than other crimes to which they compare it. Interestingly, this line of response does not appear to be dictated by the type of fraud experienced: some victims of existing account fraud and the creation of new accounts framed the incident as definitely a crime while others expressed that they saw it only as technically a crime. Relatedly, the final section of this chapter will discuss participants’ tendency to present themselves as only “technically” a victim, often when downplaying the harm incurred.
5.3.2 As Routine Inconveniences

Some participants framed the incidents as routine inconveniences rather than as crimes. Button et al. (2021) identified a continuum of perceived seriousness of cybercrime victimizations, where the lowest seriousness level is minor inconveniences, which they described as “everyday occurrences to be expected in modern life” (p. 141). Some participants who framed their experiences as inconvenient or inevitable also admitted the incident was technically a crime but downplayed its seriousness relative to other crimes.

Phoebe, a university student, was studying for exams when her bank notified her that her credit card was misused. She was eventually reimbursed, but when discussing the incident, she said: “…It was just kind of an inconvenience, right? It’s not like I lost a house or something, I just…especially if it’s during exams, it’s like, ‘I don’t need this…’ [laughs].” Similarly, Regan expressed:

Honestly, it was stressful the day of, but I had complete faith in the companies because it was clearly not my fault, the addresses didn’t match up with any of the addresses I had on file so they knew it wasn't me. And they were able to deal with it.

Both Phoebe and Regan recuperated losses by contacting banks or companies, and both framed the incidents as inconveniences that could have been worse. Nonetheless, they both also described extreme stress prior to resolving the incidents, with Regan calling the process of recuperating her stolen phone number an “absolute shitstorm.”

Importantly, some participants who saw the incident as a crime also framed it as a minor inconvenience. Jake, a marketing professional who experienced credit card fraud, understood the incident as a crime, but also added:

As long as you're not committing fraud and, you know, phoning in fake things like this then you shouldn't have any problem, you know, recovering your money. And
it’s a bit of a pain in the ass to have to replace your cards, but there's a lot worse that can happen.

Most participants who described the events as minor inconveniences did not perceive them to be serious incidents. In contrast, those suffering out-of-pocket losses and those victimized by family members did not describe incidents in this manner.

5.3.2.1 As Inevitable

Tied to understanding these incidents as inconveniences, many participants described the inevitability of identity theft in present-day Canada. The statements surrounding the inevitability of identity theft included both that there will always be motivated offenders and that breaches and hacks are inevitable with modern payment systems.

Phoebe described seeing credit card fraud as inevitable given the existence of individuals prepared to act criminally:

I think it’s becoming a more prevalent issue because more and more people are looking for a way to make like, easy money or a fast buck, so if they can figure out how to skim, just like a couple dollars off of everyone’s….like their credit cards or accounts and easily get away with it, then why wouldn’t they?

From this perspective, the inevitability of identity theft results from motivated offenders who take advantage of current technologies.

Other participants described identity theft’s inevitability in the context of society’s increased reliance on the internet and electronic payment systems. Peter is a high school student whose login information was compromised after his Spotify account was hacked. His information was then misused to gain access to his Amazon account, where fraudulent purchases were made. When describing the hack on his Spotify account, Peter said: “information leakage is, I think it’s a very ordinary thing nowadays.” Regan provided another example and stated:
“unless you're one of the most skilled firewall builders in the world, there's always going to be some modicum of risk for online stuff.” Finally, Logan, who was victim to credit card fraud, stated:

I think I kind of include it in the cost of doing business in a digital age. It's like it's bound to happen at some point. You know at some point, I mean, the digital currency will be hacked and the credit card account card will be compromised. And it's, you know, I think just a fact of life.

These quotes frame identity theft as an inevitable consequence of reliance on electronic payment systems. Tied to the framing of these as inconvenient events, these statements suggest that some victims normalized breached accounts and unauthorized charges, while trusting that companies would resolve them.

5.3.3 As Institutional Failures

Victims also framed the incidents they experienced as failures related to institutions’ security or procedures. This arose in three types of incidents: when institutions’ databases were compromised resulting in the misuse of participants’ information, when institutions were perceived to have allowed perpetrators to access the victim’s information or accounts too easily, and when participants thought unauthorized activity resulted from mistakes.

Peter framed his experience as an institutional failure after a company’s database was breached. He first noticed unusual activity with his Spotify account, then found information online suggesting the company had been hacked. Despite his personal information being used to make purchases through Amazon, he blamed Spotify, and stated: “technically, it's their fault that they let the information [leak] out.” Similarly, Edward had experienced a prior incident where his gas station loyalty points were breached and misused. Edward had researched the incident and found forums online discussing similar experiences:
I think this [Gas Station] issue, I'll call it, has been ongoing. I still follow that thread and it's happening all across Canada. It’s the [Gas Station] issue. For some reason they don't have a really good security for their website, so I'm not sure how, but these hackers manage to get in and steal your password.

In both of these cases, the victims searched for more information online and discovered that their incidents related to widespread company breaches. In turn, they both framed the incidents as institutional issues.

Other participants who framed the incident similarly described flaws in the institutions’ procedures. Although Sydney framed the misuse of her health information as a crime, she also came to understand the incident as an institutional breach of confidentiality since the perpetrator was an employee who accessed a health database:

I started realizing like how serious it actually is that [the perpetrator] had access to my health records… that’s like a breach of confidentiality… I don’t know how you can trust your healthcare system after that and stuff, especially when I’ve gone for like, serious things.

During her narrative, Sydney also expressed frustration with the institution for not addressing the breach earlier and she felt that their goal was to “…protect the [perpetrator] more than like the people that they were supposed to be serving.” To Sydney, the institution’s security procedures were breached yet they appeared to be downplaying the incident’s seriousness.

Ian is in his early 40s and also framed the misuse of his bank account by his father as an institutional issue resulting from employees not following procedures. Intending to help Ian, his father was not only making deposits into his account but also monitoring the account and transferring and withdrawing funds. Ian learned that his father had his bank account number and that the staff, who knew Ian’s father, were allowing him to debit Ian’s account, despite this being illegal. When asked whether he saw this as a crime, Ian replied:
Yeah. It’s not a crime in the, judicial sense… but it’s a crime of procedure. It’s a crime that… you had somebody looking over personal information without their permission… that’s the core of it. And, the banks allowed that to happen. Even though they have-., they should have procedures not to…

Although the details of Ian and Sydney’s victimizations were relatively unique and dissimilar from Peter and Edward’s experiences, they all framed the incidents as institutional failures. This framing is grounded in participants’ expectations that these institutions would better protect their accounts or their perception that perpetrators were too easily able to access their information or accounts.

5.3.3.1 As Institutional Errors

Finally, two victims discussed the incidents in terms of possible errors made by institutions. In both cases, the participants’ understandings of the incidents were processes, which will be discussed further in the following section. Logan’s credit card was misused in an American State he had never visited. Although he said he thought the incident was a crime, he received such little information about his misused credit card that at another point in the interview, Logan stated: “…it was physically so removed from me, that I just couldn’t imagine it being a thing other than something getting mixed up in the wires, or something like that.”

Winston’s experience was unique, but he had also come to see the incident as an institutional error. Winston is an information technology professional who was victim to recurring fraudulent tax filings spanning over a decade. Initially, he was confident that the incident was a crime perpetrated by another individual. Over time, he came to see the incident as a clerical error which may involve someone with a similar name and social insurance number: “My theory right now, that because it's been reoccurring and… like with the police investigations, and my own investigations, nothing has ever come up, I think it's a clerical error.”
These examples demonstrate that participants sometimes framed incidents as errors by companies where the victim’s account was used by mistake. Thus, identity theft can be framed as institutional failures when databases are breached, when perpetrators are easily able to access specific accounts, or when institutions make mistakes with account numbers.

5.3.4 As Relational Issues and Betrayals

Finally, participants victimized by family members generally framed these incidents as relational issues. Three of the victims interviewed had their accounts misused by a parent. Ian, who understood his father used his account with good intentions, still framed the incident as a dividing rift:

Ian: I’m still finding like there’s a pressure out there that… yeah, that I still have somebody like judging me on, uh… me as a person, me supporting my family.

Interviewer: Right… And this incident obviously was a big, like a–

Ian: Yeah… a dividing rift…

Throughout the interview, Ian regularly emphasized the relational dimensions of the incident, including describing conditions that enabled the misuse of his information and the ensuing relational consequences.

Benjamin was a university student at the time of the incident and was working full-time at the time of the interview. He was victimized by his father, who took money from Benjamin’s bank account and paid bills from Benjamin’s credit card. When asked whether he saw the incident as a crime, Benjamin replied: “I don't see it as a crime. I see it more as like a breach of trust. Like a… I don't know, like a teachable moment, like do better next time, almost.” Further, Benjamin compared his experience to that of his sister, who loaned their parents money but was not paid back, adding that “she feels a similar way.” This comparison suggests that Benjamin
primarily understood the incident as an issue between family members where relational roles were not met.

Similarly, Chandler is a young adult whose bank account was misused by her mother. While Chandler had previously told her mother her PIN for specific purchases, she framed the incident as a betrayal when her mother took her card and used it without permission:

I felt betrayed because like I had trusted my mom. Like I would let her use my card and I feel like I didn't need to do that. I was trying to be helpful and then I felt betrayed because she would then use it without my permission.

At another point, Chandler said:

I always trusted my mom and obviously the fact that I had let her know my PIN was supposed to represent that trust. And then, I feel like she misused and abused the trust because she would use the information that I gave her to disadvantage me, I guess…and I feel like she betrayed her role as mother, which is, like you know, you're supposed to be able to trust your mom…and so to have her, you know, use your account without your permission, that’s—… it’s a betrayal of trust.

All of these examples illustrate that identity theft can sometimes be understood in relational terms. When framed this way, identity theft is a breach of trust between individuals with a prior relationship, where the perpetrator misuses privileged information they have about the victim, which harms the victim and jeopardizes the existing relationship.

### 5.3.5 Intersections of Dimensions

As discussed above, victims’ understandings of the identity theft incidents involve several social frameworks: criminality, inconvenience, inevitability, institutional security practices, and relationships. While there exists considerable overlap of those describing the incidents as inconvenient, inevitable, and technically criminal, victims’ definitions of their experiences can involve numerous frameworks. Button et al. (2021) described a continuum of cybercrime victims’ experiences from minor inconveniences to serious crimes but, at least in the
case of identity theft, these could be better understood as definitional frameworks that can overlap and intersect.

Winston’s case illustrates how criminality can be a separate dimension from inconvenience, as the consequences of experiencing more than a decade of fraudulent tax filings are significantly greater than minor inconveniences, despite his belief that the incident was not a crime. Similarly, Jake identified the misuse of his credit card as a crime, yet still framed the incident as a minor inconvenience. Moreover, other examples illustrate that identity theft incidents can involve multiple definitional dimensions. Ian framed the misuse of his account by his father as both a relational rift and a crime of procedure on behalf of the bank. Further, despite his father’s good intentions, Ian understood the incident in criminal terms, since he stated: “the means is totally illegal.” Similarly, Sydney’s understanding of her misused health information rests at the intersection of an institutional breach of confidentiality and a crime. In sum, the framing of identity theft by participants was often complex, involving multiple social dimensions. Some of the complexity in framing incidents stems from victims’ limited knowledge about how incidents occur and their process of discovering and defining incidents.

5.4 Uncertainty and Processes of Definitions

Victims’ understandings of identity theft incidents must be viewed as processes. Victims of identity theft rarely have complete information about the incidents they experience: they seldom are able to identify a perpetrator, only sometimes do they know how their information was compromised, and they often speculate on intent and the cause of the incident. In survey responses, six participants indicated that they had no idea how their information was obtained, while others clarified during interviews that they were not completely certain. As such, defining
incidents was sometimes a process of discovering information. Upon first noticing a fraudulent transaction, many victims felt panic and assumed the worst before realizing that the incident was manageable. Other experiences were characterized by first noticing minor irregularities and only later realizing that one’s personal information was misused. Finally, some participants reframed incidents when they discovered new information.

A lot of the participants I spoke to described an immediate peak in emotional distress upon noticing an unauthorized charge or account takeover, due to their uncertainty of what information had been compromised and their fear of potential consequences. In the case of Ian, he noticed unusual transactions and assumed his account had been hacked. Ian expressed that until getting to the bank the next morning, “you’re panicking… and finding out what’s happening and what’s going on.” Reporting to the bank offered Ian some initial relief that no further incidents would occur. Once the bank indicated that the transactions originated from a branch in his hometown, this new information provided further relief. After realizing the perpetrator was his father and that bank employees were allowing his father to transact on Ian’s account, Ian came to define the incident in terms of a relational rift and an institutional procedural issue.

Most victims did not know their perpetrator and thus had similar initial distress but still faced uncertainty even after attempts at resolution. Marshall, who works in the telecommunications industry, was victim to a phone porting scam. These scams involve the perpetrator illegally porting (or, transferring) the victim’s phone number to another carrier in order to gain access to the mobile account. Marshall had some prior knowledge of phone porting
scams due to his employment, but also performed a Google search and knew that there was a possibility that the accounts attached to his mobile phone could have been compromised:

So essentially, the first I thought was, this is what’s going on right now: someone’s ported my number out, they’re going to try to start resetting my passwords and take control of my bank account and my credit card and my PayPal or my phone account or my e-mail account, social media accounts, and I mean, once they kind of have that, they basically have your whole life… I mean [laughs]… they’ve got everything.

Several participants reported “panicking” or “freaking out” upon realizing that an account had been compromised. Marshall eventually retrieved his phone account prior to these linked accounts being accessed, which helped to relieve distress. Nonetheless, because of the perceived intent of the perpetrator, he still identified the incident as a crime: “It was clearly an attempt to take over, you know, something to get access to something else.” Similarly, Jake, whose wallet was stolen, was called by one credit card company to indicate that it had been misused in a suspicious transaction. Jake immediately realized his entire wallet was taken and feared for his other accounts and credit cards: “I knew that I also had other cards in there and that they hadn’t called… so I presumed, in those situations, I don't know about other people, but I always presume the worst.” When he checked his other accounts and noticed only minor charges on one other credit card, he experienced some relief. However, upon learning that the cards were taken and misused near his workplace, Jake saw the incident as a crime that impacted his feelings of trust in his community. The initial panic many victims felt often subsided as they gained new information or contacted institutions who could freeze the compromised accounts.

In contrast, some victims gradually came to realize that something was wrong. In these cases, the incomplete information was usually that the participant had noticed some irregularity but not yet an unauthorized charge or transaction. Peter had multiple accounts compromised,
which he suspected began with his Spotify account being breached. Initially, Peter noticed unusual songs being played on his account:

I have never listened to that song ever. So, I just didn't think much of it. I thought someone else, some of my friends might have been using my phone to play songs, or something else… but then when I try to skip that song… it didn't skip but it stayed on the song.

Changing the password on his account appeared to correct the issue, but Peter decided to seek further information by searching the internet for his own e-mail address:

I just simply went on my… account management page and then changed my password and everything, and everything just kind of goes back to normal after that, but the story doesn't end there… so I was curious to why it happened to my Spotify account and I Googled my email address… I saw like it was an anonymous note page that people can kind of anonymously post information online. So, it was usually credit card data and stuff that was usually posted on that page. And you can actually see my password [laughs]… you see? That was when I realized this is bad.

It was at this point that Peter came to understand that something was wrong, and he proceeded to change his password on all of the accounts he could think of that used that e-mail and password combination. This demonstrates that performing an internet search can change one’s understanding of an incident.

Edward’s experience with the misuse of his Amazon account was somewhat similar in that he witnessed unusual activity prior to concluding a crime was occurring. As stated, this victimization resulted from Edward’s computer being breached while beta-testing software. He had Amazon open on his browser and gradually noticed that the list of last-viewed items were all expensive ones that he had not viewed. Edward described experiencing this process:

I'm like, ‘Whoa, what's going on?’ So, I thought maybe like at the time my girlfriend was shopping… but it didn't seem very likely that she'd be ordering this much stuff. So then, I called her, I’m like ‘Hey, are you on my Amazon account by any chance?’ She's like ‘No.’ So then I'm getting really, really worried. So then, as I go into my Amazon account, it logged me out. It said your password has been reset. And I'm
like, ‘Oh my gosh’ [laughs]. I’m like in the middle of it, I'm like watching it as it happens.

In this case, it was not until Edward was logged out of his account that he realized it had been taken over. Eventually, when he regained access to his account, he could see the address to which the items were shipped. This added information solidified to Edward that the incident was a crime.

Finally, some victims changed their perspective over time to define incidents as non-criminal or redefine incidents in other ways. Often, these changing definitions related to a lack of information known by the victim about their breached account with an institution. This can be seen in Peter’s experience, as later internet searches revealed the breached Spotify account to be a widespread company issue. Similarly, Edward found out through a forum post that his second victimization, the misuse of his gas station loyalty account, was an institutional failure causing many breached accounts. Additionally, Winston, who originally understood the misuse of his social insurance number as a crime, came to see it as a clerical error. The issue began when another individual filed their taxes under Winston’s name and social insurance number. When asked about his initial thoughts about the incident and the perpetrator, Winston expressed:

I remember at first I was-, I was just fuming angry. I really was like in my mind it was someone else. It was someone I might have worked with who had this opportunity to grab the SIN.

His perspective changed gradually as he gained new information, leading him to define the incident as an institutional error. Winston described the information that led to his changed conceptualization of the incident:

I think it was just from the gathering resources and what we could find, especially that nothing malicious was happening. Like, you’d think if someone had this… all this information to my life, they’d be quickly opening up credit cards to spend money
and never pay it off. But like, that wasn't happening. This has been very routine and almost expected now, that led me to believe like, ‘Well I don't think this is a malicious person, this is an error that's happening somewhere along the line.’

As will be discussed in the subsequent chapter, Winston reported to government organizations, police, and credit bureaus to attempt to solve the issue. The investigations largely proved unfruitful; although a Canadian tax center was able to correct the filings, the cause of the issue had yet to be confirmed and the issue continued to reoccur. However, as the incident reoccurred without further misuse of Winston’s social insurance number or identity, he gained information that led him to view the incident as separate from identity theft: had the perpetrator had access to his information, they would likely have used it for other fraudulent reasons. These examples demonstrate that understandings of identity theft incidents must be understood as processes tied to the knowledge victims have about the perpetrator, the location of charges, and the cause of incidents.

5.4.1 How Discovery and Messaging Informs Conceptualization

Part of the process of conceptualizing identity theft is victims’ interactions with institutional actors. For instance, participants who experienced credit card fraud and were made aware when a financial institution notified them were more likely to frame the events as minor inconveniences and as inevitable. These definitions may result from a perception that the bank will handle it. Phoebe stated that being notified by the bank was reassuring. Although the timing was stressful, Phoebe expressed: “…that was the first time it ever happened to me… so I wasn’t completely sure what I was supposed to do. So I just called them back and they ran through everything for me.” Jake’s case of credit card fraud was relatively unique, since being notified by
one credit card company caused him further distress as he realized his entire wallet was missing, including other debit and credit cards.

Moreover, some victims explicitly identified that their interactions with institutional actors informed how they defined incidents. Sydney found out about her misused healthcare information when she received a letter from the institution. She described not knowing how to react upon first receiving the letter: “like at first when I got the letter, I found it kind of funny.” It was not until days later that Sydney found the incident to be upsetting because of the perpetrator having access to her health records. I responded by saying that sometimes emotional reactions can take days to flesh out, and Sydney added:

Mhm. And I think also, the way that they wrote the letter was like very casual and stuff so until I started thinking deeper about like what they actually might be hiding instead of playing it off and everything, then, yeah, my opinion on it changed.

Sydney described changing her opinion and taking the incident more seriously as she interacted with other victims of identity theft who highlighted how serious the breach of personal information could be. With time, she began to think that the institution wrote the letter with the intention of protecting the perpetrator or saving their public image. This example illustrates that the way an individual discovers an incident influences their perception, particularly when they are notified by a company who may craft the message to downplay the event’s seriousness.

Logan’s definition of the credit card fraud he experienced also relates to his interactions with institutional actors. He first noticed an unauthorized charge from a US State where he had never been and assumed the incident was a crime. However, after calling the credit card company and discussing with a representative, Logan indicated that the employee’s response,
combined with the fact that only one unauthorized charge was made, led him to question whether it was a crime. I asked him if he considered himself a victim of crime, and Logan replied:

Yeah, you know, I definitely think it was a crime, but just the fact that [the bank] kind of swept it under the rug, kind of made me think maybe it was a mistake. But, you know, it just seemed kind of odd to me, that they just went after that one thing. I mean, was it a little mistake or was it a crime? I think it’s a crime more so than a mistake, but I, I don’t know. Yeah, I’ll never know. Yeah.

The subsequent chapter will discuss the common theme of participants’ feeling a lack of closure about incidents, even when they are resolved successfully, due to institutions providing little information about their nature. In this case, Logan stated that he will never know if it was a crime; the information available did not allow him to definitively conclude either way because he could not know what occurred to allow the charge to be authorized. It is common for victims to lack information about how transactions occurred or where their account or identity information was compromised. This has implications for victims’ ability to protect themselves from future incidents. The cases of both Sydney and Logan illustrate that the way institutions present information to victims can influence how they conceptualize the events.

5.4.2 Comparisons to Other Cases of Identity Theft and Fraud

Finally, part of the process of defining incidents includes the comparison of one’s experience to other identity theft cases or to common depictions of identity theft. This can be seen in Sydney’s case, where she compared her misused health information to her mother’s credit card fraud, but also in the cases of Courtney and Amanda.

Courtney is a university administrator who experienced multiple forms of identity theft. Most notably, she had ten to fifteen credit products, including credit cards and retail financing plans, opened in her name. In reference to this incident, Courtney expressed: “…you know this
isn’t like some kind of Ponzi-scheme-level fraud going on here. This isn’t, you know, this isn’t that big a deal…” The process of closing numerous credit products at different institutions took Courtney a lot of time to resolve in addition to the stress of having over $10,000 in fraudulent credit products taken out in her name. Nonetheless, she framed the incident as technically a crime but as non-serious relative to other well-known forms of fraud.

More recently, Courtney experienced fraud on her existing credit cards. With the experience of having new credit accounts created in her name, Courtney came to perceive the more recent credit card frauds as minor inconveniences:

   I would say, like, they’re not ones that freaked me out, and when the credit card company phoned and said ‘Hey, it looks like this has happened, we just need to verify some transactions,’ it doesn’t alarm me at all.

Thus, the process of defining identity theft can involve comparisons to fraud in the media or to an individual’s own prior experience with identity theft.

The case of Amanda also demonstrates the role of comparison in defining incidents. Amanda is a recent university graduate whose social media account was taken over and misused to impersonate her. She stated that she did not consider herself a victim of crime because she saw the perpetrator as a “troll.” I then asked if she considered the incident to be identity theft, and the exchange illustrates how her perception of identity theft related to cultural depictions:

   Interviewer: Do you consider that identity theft?

   Amanda: Uh, when you say identity theft, I think of the movie with Melissa McCarthy [laughs], um, I don't know if you’ve watched that, but it’s like…

34 This incident fits within the NCVS – ITS inclusion criteria as the misuse of an existing account. Nonetheless, this incident is unique and could also be framed as a form of cyberbullying. However, because Amanda does not know who her perpetrator was, the framing of this incident is likely to relate to one’s assumptions about the perpetrator’s intentions.
Interviewer: I have not, but I'm thinking I should.

Amanda: You should. Um, yeah, and just like making fake IDs, and pretending to be you, and taking out loans, and yeah like, you know maxing out your credit cards, that’s what I think of like identity theft. You know? So yeah, I don’t really think it’s identity theft.

This was the first time the term “identity theft” was used during the interview. When presented with the question of whether she considered her experience to be identity theft, Amanda quickly identified that she associated the term with more serious incidents. The meaning that Amanda associated with identity theft was therefore not compatible with the incident she experienced.

In sum, identity theft victims’ understandings of the events should be viewed as processes. Not only do victims gain information as the incident unfolds, but the messages received from institutions can influence how victims think about the events. Victims can also have incomplete information about incidents after contacting institutions for assistance. Finally, victims’ definitions of their case may be informed by comparisons to their past experiences, incidents experienced by others, or cultural depictions of identity theft.

5.5 Victims on Selves

Just as participants varied in whether they saw the incident as a crime, they varied in whether they saw themselves as victims. The way that participants framed themselves often reflected their framing of the overall incident. Although most participants acknowledged that the victim label was suitable to describe them, few readily accepted or identified with the label, with some stating that they only technically considered themselves victims. Instead, to varying degrees, many participants resisted self-labeling as a victim, instead rationalizing the events. In the context of domestic violence, Ferraro and Johnson (1983) identified several techniques of rationalizations used to normalize incidents of violence, which can be applied to other forms of
crime. Those who experienced identity theft used two such techniques to rationalize why they did not merit a victim status: denying the harm done and denying that the incident was a victimization. Further, participants often referred to typical victims of identity theft as naïve, non-technologically savvy, or otherwise vulnerable: conceptions which were sometimes enacted in comparison to one’s own experience to downplay the harm faced. Prior to discussing these groups further, it is important to note that participants’ self-definitions also changed along social dimensions other than criminality.

The intersections of crimes, inconveniences, institutional failures, and relational issues related to victims’ self-perceptions. For instance, some participants identified as victims of institutional failures, including Sydney as a victim of a breach of confidentiality and Ian as a victim of a crime of procedure. Winston, whose experience with fraudulent tax filings demonstrated the process of defining incidents, also experienced changes in his self-definitions. Winston stated:

When it first happened, I felt much more like a victim than I do now, in the sense that it's like, I felt someone was wronging me before, now it's more like the system is wronging me…

Finally, two participants identified changed relational roles as a result of the incident. Ian referred to how the incident changed his role with respect to his parents:

I can’t look at them the same way I used to. I’m almost on a defensive now, like… the roles are changing in a way. Where I am monitoring them. I’ve become the parent. I am finding out, like, ‘What are you doing now?’ or like ‘Why are you doing this?’ Um… so the roles all of a sudden hit a shift in my thirties where they were always looking after me… and all of a sudden I’m finding out how their behaviours and my behaviours are now clashing and there’s a shift in roles because of that. Where I can’t trust them- I can’t trust their behaviours so I have to, almost monitor and take decisive actions based on them, where I’ve almost become a parental… unit in a way…where I’m finding out like ‘Oh, why didn’t you pay the bills?’ or ‘Why
did you pay 200 dollars for this Rogers package?’ So I’m looking at their behaviours and monitoring them… questioning their choices…

Benjamin reported a similar shift in familial roles after the incident with his father, where he had come to see himself as more independent and prone to monitoring his younger siblings. In his case, the misused funds were received from a student loan. He stated: “Yeah, like when my sister was dealing with OSAP [Ontario Student Assistance Program] and all that I was, like, watchful, I guess…try and make sure everything was going well.” These examples demonstrate that after experiencing identity theft, participants’ self-definitions were not only related to criminality, but also to institutions and their families.

Finally, throughout the interviews, participants framed themselves as customers during specific interactions following victimizations. When discussing his disappointment with a food delivery company, Grant expressed: “I would have just hoped that they would have had a better procedure in terms of how to deal with things and how to at least reassure customers.” Unlike Winston, who compared his whole experience to an exacerbated customer service issue, these self-labels related to specific interactions with companies and financial institutions.

5.5.1 Victim Status

As noted, some victims fully accepted the victim status, which often overlapped with those who defined the incident as a crime. Edward, in describing his online shopping account being misused after beta-testing, framed the incident as a crime and gave considerable thought to the perpetrator. When asked if he was a victim of crime, he simply replied “Yes.” Additionally, although participants did not use the term “victim” unprompted while self-defining, they sometimes used the term in passing. For example, Edward had previously used the term “victim” when talking about the software company for which he was beta-testing: “They published after
that beta that… the update was broken so they pushed another update. But then yeah, I already fell victim to it so…” Similar to the terms “identity theft” and “identity fraud,” the term “victim” was omitted from recruitment materials.

Dalton was also quick to reply affirmatively when asked if he was the victim of a crime. He had used criminal terms unprompted and had called the police while attempting to resolve the incident. Jake, who was uncertain whether his credit cards were stolen from him or left somewhere and picked up, also identified as a victim. When asked if he considered himself such, Jake replied:

Yeah, absolutely… I mean, it's weird in a way because it's not like it was physically stolen from me. So, maybe I wouldn't think of myself as a victim of theft, but you know, someone's spending my money without my consent, I'm definitely a victim of a crime.

These cases demonstrate that some participants fully accepted the victim label, which was often tied to their confidence in defining the incident as criminal.

5.5.2 “Technically I Was, But…”: Resistance to the Victim Label

Many victims understood the legal definition of the term “victim” applied to them but did not identify with the label or did not feel strongly about applying the term to themselves. This often involved the denial of harm, which is one method of rationalizing incidents (see Ferraro and Johnson 1983). For example, Kathryn was eventually reimbursed after the misuse of her existing credit card. She said she would not use the term “victim of crime” herself because she felt like there are comparatively worse crimes that one could experience. Participants within this category often referred to how the incident was resolved efficiently and without suffering out-of-pocket losses or referred to other victims who faced greater repercussions.
Only two participants suffered out-of-pocket losses from their identity theft victimizations: Benjamin, who was victim to bank and credit card fraud by his father and did not view himself as a victim, and Dalton, who was victim to new account fraud by a stranger and did identify as a victim. In Phoebe’s case, recuperating losses played a role in her identification as only “technically” a victim. Phoebe was notified by her credit card company about the fraud and was eventually reimbursed. In response to asking whether she was a victim of a crime, the exchange went:

Phoebe: Like technically I was, but I wouldn’t really call myself a victim, because it was resolved and it didn’t, like, affect me that much in the long term.

Interviewer: What do you mean technically? You would be one…

Phoebe: Like, yeah, they stole something from me… so I am a victim because they stole from me, they took my personal information and used it without my consent, but I don’t feel like a victim over it because I got it all back and it was all resolved.

In this case, Phoebe did not fully embrace a victim status as the credit card company reimbursed the potential financial losses. Similarly, Amanda, who framed the incident as “trolling,” expressed that she did not see it as a crime because she did not face financial costs:

…I feel like, if I had lost money, like if they had accessed data from other websites and basically build a profile of me, to pretend to be me, like to credit card companies and what not, I would think that it would be a crime, but since it wasn’t, I didn’t lose any money… yeah, I don’t think it would be a crime.

Similar to how Amanda compared her incident to the film *Identity Thief*, she described that had she lost money or had new accounts been opened in her name, she may have viewed the incident and herself differently.

Finally, Nolan’s response to questions about the incident and himself demonstrates how the “technically” response can relate to both the resolution of the incident and how other victims
have it worse. Nolan’s credit card was misused at a bar, and although he did not seek assistance immediately, he was eventually reimbursed. When first asked whether he considered himself to be the victim of a crime, Nolan expressed:

While I would say I am the victim of the crime, I would say like, it’s not a major crime, and like, it got resolved really easily and really quickly, so uh… I don’t hold too much like, anger or whatever over it… I’m just like, it was frustrating in the time, but it’s all fixed now kind of thing.

In this case, the incident being “fixed” included Nolan having recuperated the funds taken from him. This illustrates that Nolan may have been more prepared to identify this as a major crime and accept a victim status had he not resolved the incident so quickly. The rationalization that one is not a complete victim because of a relative lack of harm was therefore common amongst participants, despite variations in the non-financial harm they experienced. For example, while Nolan reported only mild distress and resolved the incident in under a month, Amanda, who drew from similar rationalizations, reported severe distress and spent over a month resolving the incident.

5.5.3 **Comparisons to Typical Victims of Identity Theft**

In some cases, the denial of harm was tied to participants’ conceptions of typical identity theft victims. In their contributions to labeling theory, Link (1987) and Link et al. (1989) argued that individuals’ prior conceptions are integral in determining whether one will internalize or resist a self-label. Throughout the interviews, participants frequently referred to other victims of identity theft using stereotypical descriptors as old, naïve, or non-technologically savvy. Similar to past research in Australia (see Cross 2015), these depictions imply that identity theft victims are perceived as having some responsibility for their own victimization, either by falling for a scam or by not knowing how to protect oneself.
When discussing victimhood, participants brought up other victims of identity theft when comparing their situation to those who had it worse and when comparing themselves to those who were more vulnerable to victimization. As an example of the typical construction of identity theft victims, Nolan, a university student, stated he did not previously think he would experience fraud because: “most people don’t think they’re like dumb, basically, you’re like, ‘Oh I would never fall for like a scheme like that, or a scam or something…’.” Later, when discussing his victim status, Nolan compared himself to other potential victims:

I don’t know if I would call myself a victim really, I would say like someone who had like 20 thousand dollars taken from their account or like a house payment bounce because someone used their stuff to buy stuff online would definitely be more of a victim than I am. Like… it’s kind of tough to say everyone’s a victim in the same sense… like there’s more vulnerable people that have dealt with more trouble than I have, for sure. So, I wouldn’t necessarily like, go around, like ‘Oh, I’m a victim of identity theft’ kind of thing, because like people have had it worse.

In Nolan’s opinion, his incident was not sufficiently serious to self-identify as a victim. He also referred to how some victims may be more vulnerable, which could relate to stereotypes of victims who are unable to protect themselves.

Grant, who is in his late-20s, compared himself to an older victim of identity theft in the case of his misused food-delivery account. He brought up an incident involving an individual he knew who was victim to a common Canadian scam where perpetrators pose as the Canada Revenue Agency (CRA) and threaten legal recourse if the victim does not reply. Grant described that this individual:

…was a victim of one of those telephone scams… where they call and they say, ‘We’re calling from the Canada Revenue Agency and you need to remain on the phone or we’re going to, you know, dispatch the police to your house.’ So like, we were all kind of like, ‘You really thought that was Canada Revenue Agency, like are you serious?’ [laughs] Um, but anyway, he’s in his sixties.
This quote illustrates the use of humour which was common when describing victims who fall for scams. Further, it shows an attitude that falling for such a scam can be explained, in part, in terms of the victim’s age. At another point, Grant stated that he had not thought he would be victimized as he “incorrectly assumed that like, you need to be kind of naïve to fall victim to this sort of a scam.”

While discussing this older victim, Grant proceeded to state: “Yeah, so, anyway, I just compare my situation, where I was able to recuperate all my money, I was able to like, you know, be assertive with the people on the phone.” Further, during Grant’s interview, he used the term “victim” unprompted when describing the individual who experienced the CRA scam. Later, when asked whether he considered himself a victim, he stated: “Um… no, because I never really thought about it.” After each of us laughing, Grant proceeded to describe how he technically fit the definition but would not apply the term to himself:

I mean I think… if you asked me like, as per a textbook definition of like, you know, who is the perpetrator, who is the victim, technically speaking I am the victim in this situation …but I would not have defined myself as such, you know, before the question was asked to me.

In this case, Grant did not directly compare his experience to others when asked whether he identified as a victim, but he did when comparing their ability to resolve incidents. Nonetheless, his use of the term victim in the context of the other individual but lack of thought about it in terms of himself demonstrates resistance to the status. However, not all of those who held prior conceptions of victims as naïve or vulnerable resisted the term. For example, Edward stated that he had previously not believed he would be victim to identity theft because he was “security-minded,” yet he accepted the victim label. Overall, comparisons to other and typical victims of
identity theft can be a way of rationalizing the incident as relatively unharmful, thus resulting in resisting full status as a victim.

5.5.4 Self-Blame and Denying a Victimization Occurred

Few participants outright denied a victim status; 35 when they did, it was sometimes tied to self-blame. Self-blame, or accepting some level of responsibility for an incident, can be a method of rationalizing incidents by denying that the event was a victimization (see Ferraro and Johnson 1983). Participants reported varying degrees of self-blame, with some recognizing that they could have avoided sharing personal information and others referring to ways that they could have better secured their accounts. Self-blame can also relate to common depictions of identity theft victims, since victims are often viewed as naïve for falling for a scam or non-technologically savvy and not protecting oneself adequately.

Benjamin and Chandler, who were victimized by family members, both expressed self-blame for having trusted the perpetrator with information and both denied a victim status. Benjamin’s student loan funds were misused from his bank account. When discussing ways to prevent the incident, Benjamin said: “…in a way like, I kind of almost let this happen.” Later in the interview, Benjamin expressed that: “It felt like a three strikes and you’re out moment for me and that was like the first strike… when, you know, one strike is enough.” Benjamin did not view himself as a victim or the incident as a crime, instead framing it as a “teachable moment” and a “breach of trust.”

35 Some past research has indicated that despite potential benefits of the victim label, it can also be associated with weakness (see, for instance, Fohring 2018). Although Regan stated that the incident “wasn't anything I couldn't handle,” participants who resisted the term did not volunteer associations of the term with weakness. Further, an analysis of differences in acceptance and resistance of a victim status between genders did not reveal discernible differences in perceptions of the term itself.
In the case of Chandler’s misused bank account, she expressed: “It’s both of our faults. It’s my fault for letting her know my PIN and it’s her fault for using it without my permission.” Despite letting her mother know her PIN, the expectations based on their relationship were that the PIN would not be misused and Chandler’s debit card would not be taken without her permission. When initially asked whether the incident was a crime, she responded: “technically, I guess, yeah.” However, she primarily framed the incident as a relational issue and expressed that she never thought of it as a crime. When asked if she had thoughts about the use of the term “victim” in this context, Chandler replied:

I wouldn’t say that I was a victim, I was just stupid because I was the one who let her know my PIN and so it’s like, it’s-, I’m not a victim, like I’m-, I’m partially responsible.

Here, Chandler framed her response to suggest that holding some responsibility for the incident precluded her from identifying as a victim. In both Benjamin and Chandler’s case, having trusted the perpetrator with personal information meant rejecting the victim status by denying that a victimization occurred due to the responsibility they attributed to themselves.

Other cases where participants did not know their offender but provided information to perpetrators resulted in self-blame. For example, Hunter’s most recent experience with credit card fraud was the result of a phishing scam, where someone posed as a company asking them to update their credit card information. Hunter expressed:

… the second one I just felt stupid, like I was like, ‘How could this have happened?’ Like, it looked so legitimate and then, I don’t know... like, you know when you hear about people, older people and kind of like CRA things happening to them, I was like, ‘Oh my gosh, like, I feel like, I’m an old person, who’s struggling [laughs] with this.’
In this case, Hunter did not feel strongly about whether the incident was a crime, stating: “Um, yeah, I mean, I guess it is, right?” In addition to comparing their experience directly to their prior conception of identity theft victims, Hunter also described having felt somewhat responsible for the incident. Similar to Chandler’s case, individuals can rationalize incidents by describing that the victimization could have been avoided had they taken different actions. Hunter’s case illustrates how self-blame can also relate to comparisons to typical victims of identity theft.

In sum, although some participants viewed themselves as victims, many resisted victim statuses by rationalizing the incident in multiple ways. Some victims denied a victimization occurred and instead blamed themselves; this was common in cases where the perpetrator was known or when the victim provided information to a perpetrator. Similarly, some rationalized the incident to varying extents by comparing their cases to other victims they deemed to have had worse outcomes or who were otherwise more vulnerable, thus denying the harm experienced. This sometimes involved comparisons to stereotypical victims who are naïve, old, or non-technologically savvy. In cases where victims recuperated losses, these rationalizations framed the victim as relatively fortunate in comparison to others, which neglected the non-financial costs of identity theft incidents.

5.6 Summary

In summary, I argue that identity theft incidents are conceptualized by victims to exist at the intersection of several social frameworks. Thus, the answer to the first research question regarding how victims understand incidents is that they may define them as criminal actions or inevitable inconveniences associated with modern payment systems, or as institutional failures or relational issues. Further, similar to Button et al.’s (2021) argument that experiences of
cybercrime victimization exist on a continuum of seriousness, these findings suggest definitions of identity theft may be even more complex, with some participants framing incidents using definitional terms from multiple social frameworks. Like all social objects, the definitions of these incidents should be understood as processes. Identity theft victims often have incomplete information about the nature of the incident, their perpetrator, and how their information was breached; as they gain new information about the nature of an incident, they may reframe the events. Additionally, communications with institutional actors and comparisons to other incidents inform victims’ definitions of identity theft incidents.

With respect to victims’ understandings of themselves following identity theft victimizations, self-definitions often relate to how victims define the incident itself. Some participants viewed themselves as victims, while others framed the self using non-criminal definitions, including as victims of institutional failures or as taking on new familial roles. When confronted with the victim label, some participants admitted that they were “technically” victims, but would not identify as such for several reasons, including that others have experienced worse consequences or that the incident could have been prevented. Participants frequently held prior conceptions of typical identity theft victims as naïve or old and sometimes compared their experiences with these conceptions in downplaying the seriousness of the incident. In some cases, participants described themselves as having some role in the victimization, which could lead to resistance of the victim label by denying that a victimization occurred. These rationalizations can overshadow the costs that victims face.

The subsequent chapter presents findings regarding victims’ reporting decisions following identity theft incidents. Quantitative analysis of the NCVS – ITS estimate trends in
factors related to reporting and whether suffering out-of-pocket losses moderates the effects of other measures of seriousness. Qualitative analysis of the interviews indicates how definitions of incidents and the self relate to reporting decisions. Finally, the chapter will discuss participants’ experiences and satisfaction with these institutions.
6 Results 2: Victims Reporting Decisions and Experiences with Reporting

6.1 Introduction

The previous chapter argues that victims’ understandings of identity theft and themselves are processes. The process does not end with reporting to institutions; rather, new information can be gained from institutional actors that further impacts victims’ understandings of the events experienced. Moreover, reporting decisions are processes, with the advice provided and resolutions facilitated by one institution influencing subsequent decision-making by victims. Unlike some crimes, police do not have a monopoly on responding to identity theft. Instead, credit card companies, banks, other private companies, and credit bureaus all play a role in identity theft’s security landscape.

This chapter examines this study’s second and third research questions. The chapter first examines to whom identity theft victims formally report and why. To answer this question, a quantitative analysis of the 2016 United States National Crime Victimization Survey – Identity Theft Supplement (NCVS – ITS) examines factors influencing victims’ decisions to report to police, financial institutions, and credit bureaus. Further, drawing from interviews, this chapter examines participants’ reasoning for their reporting decisions. I argue that participants’ reporting decisions often related to their framing of incidents. As such, many reported only to the extent necessary to recuperate losses, although external advice and emotional reactions, including embarrassment, also influenced decision-making. Moreover, participants rarely reported to police, often because they felt the incident was already resolved or not suitable for police, or because they felt police could or would do nothing.
The last section of this chapter addresses the third research question and examines victims’ satisfaction with the resolutions facilitated by institutions. Although some victims were fully satisfied with the institutions they contacted, I argue that many victims experienced frustration and dissatisfaction with institutions for being transferred from department to department, having to call companies repeatedly, feeling that processes were not straightforward, or feeling that employees did not want to help or failed to sympathize. Finally, some victims felt a lack of closure because institutions did not provide them with information about the results of investigations and the nature of incidents.

This chapter begins by describing the 2016 NCVS – ITS sample and findings from logistic regression analyses of factors influencing victims’ decisions to notify police, financial institutions, and credit bureaus. Next, I describe findings from the interviews with victims of identity theft in Southern Ontario, including victims’ reasoning for reporting to companies and financial institutions, their reasons for not reporting to police, and finally, their level of satisfaction with the resolutions facilitated by the institutions involved.

6.2 Quantitative Results: Reporting to Law Enforcement, Financial Institutions, and Credit Bureaus

6.2.1 Descriptive Statistics

Table 6-1 displays the distributions for the variables used in this study. The summary statistics indicate that nearly 95 percent of identity theft victims who had some value of goods or services taken reported to a financial institution, while few victims reported to law enforcement or credit bureaus (6 percent each). Individually, these figures suggest that few incidents of identity theft come to the attention of law enforcement, and that collectively, banks and credit card companies are aware of most incidents. The focus of the ensuing analyses is to identify the
situational and sociodemographic factors that lead to increased reporting to each institution, which is important to better understand the characteristics of incidents coming to the attention of the security actors.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Percentage/Mean</th>
<th>SD</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reported to Police</td>
<td>5.86</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reported to Financial Institution</td>
<td>94.63</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reported to Credit Bureau</td>
<td>5.84</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Financial Loss</td>
<td>8.20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at all Distressing (Ref)</td>
<td>17.16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mildly Distressing</td>
<td>48.06</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderately Distressing</td>
<td>26.21</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severely Distressing</td>
<td>8.57</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know About Offender</td>
<td>5.77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know How Information Was Obtained</td>
<td>28.35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Made Aware by Financial Institution</td>
<td>44.86</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prior Victim of Identity Theft</td>
<td>23.22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Married</td>
<td>64.85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>52.55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White (Ref)</td>
<td>79.78</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Black</td>
<td>6.76</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td>7.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>5.75</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeast (Ref)</td>
<td>10.95</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Midwest</td>
<td>28.37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South</td>
<td>34.35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>West</td>
<td>26.33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount Taken</td>
<td>676.70</td>
<td>1637.89</td>
<td>2 – 17000</td>
</tr>
<tr>
<td>Time Spent Resolving Incident</td>
<td>One Day or Less (1.97)</td>
<td>1.14</td>
<td>1 – 7</td>
</tr>
<tr>
<td>Time Personal Information was Misused</td>
<td>One Day or Less (1.85)</td>
<td>1.07</td>
<td>1 – 7</td>
</tr>
<tr>
<td>Income</td>
<td>$40,000 to $49,999 (12.26)</td>
<td>2.90</td>
<td>1 – 14</td>
</tr>
<tr>
<td>Education</td>
<td>Some College (3.50)</td>
<td>1.13</td>
<td>1 – 5</td>
</tr>
<tr>
<td>Age</td>
<td>48.23</td>
<td>15.84</td>
<td>16 – 90</td>
</tr>
</tbody>
</table>
In terms of consequences of victimization, the average amount taken from victims was $677, with a median of $200 taken. This variable was logged prior to the analysis to account for its skewed distribution. Importantly, 8 percent of identity theft victims suffered out-of-pocket losses after attempts at recuperation. Victims reported spending an average of one day or less resolving the incident, although some spent over a year resolving incidents. Finally, while 17 percent of victims stated that the incident was not at all distressing, most victims reported experiencing mild (48 percent) or moderate (26 percent) distress, and 9 percent of victims reported severe distress.

For other situational factors, fewer than one third (28 percent) of participants knew how their information was obtained while even fewer (6 percent) knew anything about the offender. On average, participants’ information was misused for less than a day. Nearly half (45 percent) of victims became aware of the incident after being notified by their bank or credit card company. Finally, almost 23 percent of participants reported having been victim to a prior identity theft incident.

With respect to sociodemographic variables, the participants’ mean age was 48 years old, with slightly more females (52 percent) than males in the sample. The average household income was $40,000-$49,000, with a mean educational attainment of having completed some college. Nearly two thirds (65 percent) of victims were married. Most victims in the sample were white (80 percent), followed by Hispanic/latinx (8 percent), Black (7 percent), and Other (6 percent). The largest proportion of victims lived in the Southern United States (34 percent), followed by the Midwest (28 percent), the West (26 percent), then the Northeast (11 percent).
6.2.2 Reporting to Law Enforcement

Several multiple logistic regression models were estimated for each of the reporting institutions. Across eight models, reporting to law enforcement was regressed on measures of seriousness, situational factors, and sociodemographic variables. In Table 6-2, Model 1 tested the effects of measures of seriousness, while Model 2 examined the effects of situational factors. Model 3 assessed the effects of the measures of seriousness while controlling for these situational factors. Model 4 tested the effects of sociodemographic variables. Finally, Model 5 is the full model, which examined the effects of measures of seriousness on police reporting while holding sociodemographic and situational variables constant at their means or proportions.

The data in Model 1 reveal that when one does not control for situational or sociodemographic factors, all measures of seriousness were significant predictors of police reporting. Those who suffered out-of-pocket losses were approximately three times more likely to report to police than those who recuperated losses \((p \leq 0.001)\). As the amount taken from the victim increased, so too did their likelihood of reporting, with each logged one-unit increase in the amount taken predicting a nearly 50 percent increase in reporting to police\(^{36} \,(p \leq 0.001)\). Time spent resolving the incident also related to an increased likelihood of reporting to police: for each one-unit increase in time resolving the incident, victims were 1.3 times as likely to report to law enforcement \((p \leq 0.001)\). Finally, distress was also a statistically significant predictor of reporting: compared to those experiencing no distress, those with mild distress were

\(^{36}\) As this variable was transformed into a logarithmic variable due to its skewed nature, the odds ratios cannot easily be interpreted into dollar values. Nonetheless, an odds ratio of greater than one indicates that as the amount taken from the victim increased, so too did the victim’s likelihood of reporting. An analysis was performed to examine whether the amount lost out of pocket impacted the likelihood of reporting to police. The results revealed similar increases between the likelihoods of reporting for those losing under $100, $100-$999 and over $1000.
more than twice as likely to report to police ($p \leq 0.05$), while those with moderate and severe
distress were more than three and four times as likely to report to police, respectively ($p \leq 0.001$).

Model 2 estimated the effects of situational variables on police reporting, while Model 3
included both situational variables and measures of seriousness. The data in Model 2 reveal that
being made aware of the identity theft incident by a financial institution decreased the likelihood
of reporting to law enforcement ($p \leq 0.01$), while knowing about the offender, knowing how
one’s information was obtained, and reporting to credit bureaus were related to significant
increases in police reporting ($p \leq 0.001$). The direction and significance of these associations
remained in Model 3. Additionally, the length of time one’s information was misused was
negatively correlated with one’s odds of reporting to police in Model 3 ($p \leq 0.05$). When
controlling for these situational variables, the measures of seriousness were again statistically
significant predictors of reporting in the expected directions, although their effects were
dampened. Further, distress was less statistically significant ($p \leq 0.05$) in Model 3 than in Model
1, and the significance of both moderate and severe distress compared to no distress decreased ($p
\leq 0.01$).

The data in Model 4 reveal that most sociodemographic variables were not statistically
significant predictors of reporting to police. The victim’s region of the United States was the
exception, with those in the Midwest and Southern United States approximately 1.7 times more
likely to have reported identity theft to law enforcement than those in the Northeast ($p \leq 0.05$).
Table 6-2: Logistic regression predicting identity theft victims reporting to law enforcement (n = 5,753)

<table>
<thead>
<tr>
<th></th>
<th>Model 1</th>
<th>Model 2</th>
<th>Model 3</th>
<th>Model 4</th>
<th>Model 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Pocket Loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>3.081 ***</td>
<td>2.253 ***</td>
<td>2.124 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount Taken (log)</td>
<td>1.466 ***</td>
<td>1.455 ***</td>
<td>1.463 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>1.340 ***</td>
<td>1.251 ***</td>
<td>1.237 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at All</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mild</td>
<td>2.143 *</td>
<td>2.124 *</td>
<td>2.114 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>3.211 ***</td>
<td>2.526 **</td>
<td>2.593 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>4.476 ***</td>
<td>2.919 **</td>
<td>2.961 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prior ID Theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.926</td>
<td>0.895</td>
<td>0.903</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know Anything About Offender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>3.932 ***</td>
<td>2.955 ***</td>
<td>2.876 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know How Information Obtained</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>2.788 ***</td>
<td>2.310 ***</td>
<td>2.336 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Time Information Misused</td>
<td>1.002</td>
<td>0.852 *</td>
<td>0.854 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Made Aware by Financial Institution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.573 **</td>
<td>0.644 **</td>
<td>0.648 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reported to Financial Institution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.861</td>
<td>0.945</td>
<td>0.978</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reported to Credit Bureau</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>6.258 ***</td>
<td>4.35 ***</td>
<td>4.371 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td>1.009</td>
<td>1.003</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Income</td>
<td></td>
<td>0.965</td>
<td>0.984</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td>0.934</td>
<td>0.995</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Black</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marital Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmarried</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Married</td>
<td></td>
<td>0.899</td>
<td>0.944</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeast</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Midwest</td>
<td></td>
<td>1.686 *</td>
<td>1.862 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>South</td>
<td></td>
<td>1.703 *</td>
<td>1.842 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>West</td>
<td></td>
<td>1.095</td>
<td>1.217</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pseudo R²</td>
<td>0.144</td>
<td>0.141</td>
<td>0.217</td>
<td>0.018</td>
<td>0.225</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001
The estimates from Model 5 demonstrate that measures of seriousness remained significant predictors of reporting to law enforcement when controlling for other situational factors and sociodemographic variables. The effects of measures of seriousness on police reporting in Model 5 were similar to Model 3, although out-of-pocket loss was less significant ($p \leq 0.01$). Further, in the full model, the situational and demographic variables had similar significance and effects as in Model 3 and Model 4, respectively. Finally, the model fit statistics in Model 5 were similar to those in Model 3.

Interaction effects were tested between suffering out-of-pocket losses and the other measures of seriousness, since paying out of pocket may impact whether individuals see themselves as a victim of crime and may thus inform reporting decisions. In Table 6-3, Models 6, 7, and 8 tested these interaction effects while controlling for all of the situational and sociodemographic variables included above. A full version of Table 6-3, with control variables, is presented in Appendix F. Model 6 examined the interaction between the logged amount taken and out-of-pocket loss and found that the interaction term was not statistically significant. The estimates in Model 7 display a statistically significant interaction term between out-of-pocket loss and time spent resolving the incident ($p \leq 0.01$). Finally, in Model 8, the overall interaction term between distress and out-of-pocket loss was not statistically significant. Nonetheless, the interaction term between out-of-pocket loss and the dummy category severe distress was significantly different from those reporting no distress. The odds ratio of 0.15 suggests that experiencing severe distress increased reporting to police more for victims who recuperated losses compared to those who suffered out-of-pocket losses ($p \leq 0.05$).
Table 6-3: Logistic regression predicting identity theft victims reporting to law enforcement (n = 5,753)

<table>
<thead>
<tr>
<th></th>
<th>Model 6</th>
<th>Model 7</th>
<th>Model 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Pocket Loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>7.095 *</td>
<td>5.110 ***</td>
<td>7.610 **</td>
</tr>
<tr>
<td>Amount Taken (log)</td>
<td>1.527 ***</td>
<td>1.481 ***</td>
<td>1.476 ***</td>
</tr>
<tr>
<td>Time</td>
<td>1.251 ***</td>
<td>1.338 ***</td>
<td>1.240 ***</td>
</tr>
<tr>
<td>Distress</td>
<td>*</td>
<td>*</td>
<td>**</td>
</tr>
<tr>
<td>Not at All</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Mild</td>
<td>2.124 *</td>
<td>2.093 *</td>
<td>2.653 **</td>
</tr>
<tr>
<td>Moderate</td>
<td>2.581 **</td>
<td>2.517 **</td>
<td>3.380 **</td>
</tr>
<tr>
<td>Severe</td>
<td>3.022 **</td>
<td>2.928 **</td>
<td>4.767 ***</td>
</tr>
<tr>
<td>Out-of-Pocket Loss*Amount Taken (log)</td>
<td>0.818</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out-of-Pocket Loss * Time Spent</td>
<td></td>
<td>0.734 **</td>
<td></td>
</tr>
<tr>
<td>Out-of-Pocket Loss * Distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Not at All</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>*Mild</td>
<td></td>
<td></td>
<td>0.378</td>
</tr>
<tr>
<td>*Moderate</td>
<td></td>
<td></td>
<td>0.290</td>
</tr>
<tr>
<td>*Severe</td>
<td></td>
<td></td>
<td>0.148 *</td>
</tr>
<tr>
<td>Pseudo R²</td>
<td>0.226</td>
<td>0.228</td>
<td>0.229</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001
Each model controlled for all situational and sociodemographic variables tested above. For the complete table with control variables, see Appendix F.

To assist in the interpretation of regression estimates, Figure 6-1 displays the predicted probabilities for victims who suffered out-of-pocket losses compared to those who recovered losses at different levels of time spent resolving the incident. These estimates were calculated by holding all other variables constant at their proportions or means. For those victims who recuperated losses, the predicted probability of reporting to police if the incident was resolved within a day or less was 0.035. As the time spent resolving the incident increased, so too did the likelihood of reporting to police for these victims: their predicted probability of reporting was over 0.100 at six months or more and a year or more. In contrast, victims who suffered out-of-pocket losses had a relatively stable likelihood of reporting based on the time spent resolving the incident. The predicted probability of reporting to law enforcement for these victims ranged from 0.104 at one day or less spent resolving the incident to 0.096 at a year or more.
Figure 6-1: Predicted probabilities of reporting to law enforcement based on time spent resolving incidents for those suffering out-of-pocket losses and those recuperating losses

Table 6-4 presents the predicted probabilities of reporting based on out-of-pocket loss and distress, holding the other variables constant at their means or proportions. Only the interaction term for those who experienced severe distress was statistically significant. However, this suggests that variations in distress impacted the likelihood of reporting more for those who recovered losses than for those who did not. For those recuperating losses, the likelihood of having reported to police was 0.02 when suffering no distress but 0.08 when experiencing severe distress. The likelihood of reporting for those suffering out-of-pocket losses was 0.11 for those experiencing no distress and 0.08 for those who reported severe distress.

<table>
<thead>
<tr>
<th>Distress</th>
<th>No Out-of-Pocket Loss</th>
<th>Out-of-Pocket Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Margins</td>
<td>95% CI</td>
</tr>
<tr>
<td>Not at All</td>
<td>0.020</td>
<td>0.008-0.031</td>
</tr>
<tr>
<td>Mild</td>
<td>0.046</td>
<td>0.036-0.056</td>
</tr>
<tr>
<td>Moderate</td>
<td>0.057</td>
<td>0.045-0.068</td>
</tr>
<tr>
<td>Severe</td>
<td>0.075</td>
<td>0.050-0.100</td>
</tr>
</tbody>
</table>
6.2.3 Reporting to Financial Institutions

Logistic regression analyses were also used to estimate the effect of measures of seriousness and situational and sociodemographic factors on reporting to financial institutions. The eight models, displayed in Table 6-5 and Table 6-6, are presented in a similar order to those predicting reporting to law enforcement.

In Table 6-5, Model 1 presents the estimates for the effects of measures of seriousness on reporting to financial institutions. In contrast to reporting to law enforcement, suffering an out-of-pocket loss was associated with a lower likelihood of having contacted a financial institution \( (p \leq 0.001) \). The effects of the amount taken and the time spent resolving the incident were not statistically significant predictors of reporting to banks or credit card companies when controlling for the other variables in the model. Distress was statistically significant: those who experienced mild \( (p \leq 0.01) \), moderate \( (p \leq 0.01) \), and severe distress \( (p \leq 0.05) \) were more likely to have reported to financial institutions than those who experienced no distress.

Model 2 presents the effects of situational factors on reporting to financial institutions. In this model, having experienced a prior identity theft incident increased the chances of reporting to financial institutions \( (p \leq 0.05) \). Having information about the offender decreased the likelihood of reporting \( (p \leq 0.001) \), although knowing how one’s information was obtained was not a significant predictor. The greater the length of time one’s information was misused decreased the likelihood of reporting \( (p \leq 0.001) \) and being made aware of the incident by one’s financial
<table>
<thead>
<tr>
<th></th>
<th>Model 1</th>
<th>Model 2</th>
<th>Model 3</th>
<th>Model 4</th>
<th>Model 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Out-of-Pocket Loss</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.238***</td>
<td>0.318***</td>
<td>0.317***</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Amount Taken (log)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0.950</td>
<td>0.952</td>
<td>0.952</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>0.931</td>
<td>1.049</td>
<td>1.056</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Distress</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at All</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Mild</td>
<td>1.615**</td>
<td>1.628**</td>
<td>1.668**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>1.725**</td>
<td>1.904**</td>
<td>1.938**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>1.702*</td>
<td>2.168**</td>
<td>2.163**</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Prior ID Theft</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>1.453*</td>
<td>1.369</td>
<td>1.390</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>KnowAnything About Offender</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.486***</td>
<td>0.568*</td>
<td>0.554*</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Know How Information Obtained</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.920</td>
<td>0.934</td>
<td>0.941</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Length of Time Information Misused</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>0.801***</td>
<td>0.821**</td>
<td>0.814**</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.831***</td>
<td>1.846***</td>
<td>1.839***</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Made Aware by Financial Institution</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>1.001</td>
<td>1.003</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Reported to Law Enforcement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.870</td>
<td>0.956</td>
<td>0.967</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Reported to Credit Bureau</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.632</td>
<td>0.619</td>
<td>0.615*</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>1.037</td>
<td>1.008</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Income</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.989</td>
<td>0.919</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.735</td>
<td>0.876</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Female</td>
<td>0.970</td>
<td>0.927</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Race/Ethnicity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Black</td>
<td>0.971</td>
<td>0.986</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>1.065</td>
<td>1.193</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Marital Status</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmarried</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Married</td>
<td>0.987</td>
<td>0.930</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeast</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Midwest</td>
<td>0.764</td>
<td>0.693</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South</td>
<td>0.634</td>
<td>0.611*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>West</td>
<td>0.763</td>
<td>0.691</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Pseudo R²</strong></td>
<td>0.040</td>
<td>0.043</td>
<td>0.069</td>
<td>0.007</td>
<td>0.074</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001
institution increased this likelihood\textsuperscript{37} ($p \leq 0.001$). Finally, contacting law enforcement and credit bureaus were not significant predictors of reporting to financial institutions.\textsuperscript{38}

Model 3 presents the effects of measures of seriousness while controlling for situational variables. In this model, the effects of measures of seriousness were similar to Model 1, although the significance of distress, and the dummy category severe distress, increased ($p \leq 0.01$). Additionally, some of the situational variables were less significant in Model 3 than in Model 2: having experienced a prior identity theft incident was no longer significant, while knowing one’s offender ($p \leq 0.05$) and the length of time one’s information was misused ($p \leq 0.01$) were less significant. Finally, the data in Model 4 present the effects of demographic predictors on reporting to financial institutions and none of the demographic variables were statistically significant predictors.

Model 5 is the full model, producing estimates for measures of seriousness on reporting to financial institutions when controlling for situational and sociodemographic factors. The estimates and significance for measures of seriousness were similar to Model 3, with out-of-pocket loss once again associated with a decreased likelihood of reporting to financial institutions ($p \leq 0.001$), while experiencing mild, moderate, or severe distress increased the

\textsuperscript{37} Individuals are included as being made aware by a financial institution when they responded “credit card company or bank contacted me about suspicious activity on my account” to a question asking how they first found out about the incident (United States Department of Justice 2016: 180). Supplemental analysis reveals that about 5 percent of victims who were made aware by a financial institution did not indicate that they reported to a financial institution, which may suggest they did not respond to calls, texts, or e-mails they received.

\textsuperscript{38} Given the exploratory nature of this analysis and that victims may take different pathways when reporting to these institutions, the dependent variables were tested as independent variables in other models. Supplemental analysis of the models when removing the other reporting options produced similar coefficients and significance for most variables, and the overall trends in findings were similar (including interaction effects).
likelihood of reporting compared to those experiencing no distress \((p \leq 0.01\)). Similarly, the effects and significance of situational variables were unchanged from Model 3, with one exception: when controlling for sociodemographic characteristics, reporting to credit bureaus was associated with a decreased likelihood of reporting to financial institutions \((p \leq 0.05\)). Finally, although region of the United States was not a significant predictor overall, those in the South were less likely to report to credit card companies and banks compared to those in the Northeast \((p \leq 0.05\)).

In Table 6-6, the estimates in Models 6, 7, and 8 tested interaction effects between suffering out-of-pocket loss and the other measures of seriousness. In the case of reporting to financial institutions, none of these interaction effects were statistically significant, indicating that out-of-pocket loss did not moderate the effect of other measures of seriousness when predicting reporting to credit card companies or banks.

| Table 6-6: Logistic regression predicting identity theft victims reporting to financial institutions (n = 5,753) |
|---------------------------------------------------------------|--------|--------|--------|
| Out-of-Pocket Loss                                           | Model 6 | Model 7 | Model 8 |
| No                                                           | —      | —      | —      |
| Yes                                                          | 0.201 ** | 0.274 *** | 0.342 ** |
| Amount Taken (log)                                           | 0.933 | 0.949 | 0.953 |
| Time                                                         | 1.048 | 1.036 | 1.057 |
| Distress                                                     | **     | **     | **     |
| Not at All                                                   | —      | —      | —      |
| Mild                                                         | 1.667 ** | 1.675 ** | 1.657 * |
| Moderate                                                    | 1.947 ** | 1.953 ** | 2.019 ** |
| Severe                                                      | 2.113 ** | 2.157 ** | 2.303 * |
| Out-of-Pocket Loss*Amount Taken (log)                       | 1.093 |       |       |
| Out-of-Pocket Loss * Time Spent                             |       | 1.064 |       |
| Out-of-Pocket Loss * Distress                                |       |       |       |
| *Not at All                                                 | —      | —      | —      |
| *Mild                                                       | 1.025 |       |       |
| *Moderate                                                   | 0.811 |       |       |
| *Severe                                                     | 0.829 |       |       |
| Pseudo R²                                                   | 0.074 | 0.074 | 0.074 |

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001
Each model controlled for all situational and sociodemographic variables tested above. For the complete table with control variables, see Appendix F.
6.2.4 Reporting to Credit Bureaus

Finally, a series of logistic regression analyses were estimated to examine the effect of measures of seriousness, situational factors, and sociodemographic variables on reporting to credit bureaus. These are presented in Table 6-7 and Table 6-8. Again, the models are presented in the same order as the models for reporting to law enforcement and financial institutions.

In Table 6-7, the data in Model 1 display the effects of measures of seriousness on reporting to credit bureaus, without controls. Similar to reporting to law enforcement and dissimilar to reporting to financial institutions, having suffered out-of-pocket losses predicted an increase in reporting to credit bureaus ($p \leq 0.05$). As the logged amount taken from the victim ($p \leq 0.001$) and the time they spent resolving the incident ($p \leq 0.001$) increased, so too did the likelihood of reporting to credit bureaus. Finally, although distress was a significant predictor of reporting ($p \leq 0.01$), experiencing mild, moderate, or severe distress were not associated with significant differences in the likelihood of reporting compared those who experienced no distress.

Model 2 tested the effects of situational variables on reporting to credit bureaus. In this model, having experienced a prior identity theft victimization was related to a decreased likelihood of reporting ($p \leq 0.01$), while having the information misused for longer periods related to a higher likelihood of reporting to credit bureaus ($p \leq 0.01$). Finally, reporting to law enforcement was a strong predictor, leading to an over six times increase in the likelihood of also reporting to credit bureaus ($p \leq 0.001$). Model 3 presents the effects of measures of seriousness while controlling for situational variables. The situational factors had similar effects in Model 3.
Table 6-7: Logistic regression predicting identity theft victims reporting to credit bureaus (n = 5,753)

<table>
<thead>
<tr>
<th></th>
<th>Model 1</th>
<th>Model 2</th>
<th>Model 3</th>
<th>Model 4</th>
<th>Model 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Pocket Loss</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>1.577 *</td>
<td>1.215</td>
<td>1.215</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amount Taken (log)</td>
<td>1.184 ***</td>
<td>1.114 *</td>
<td>1.112 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>1.462 ***</td>
<td>1.363 ***</td>
<td>1.351 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distress</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
<td>**</td>
</tr>
<tr>
<td>Not at All</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Mild</td>
<td>0.773</td>
<td>0.757</td>
<td>0.772</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>1.362</td>
<td>0.133</td>
<td>1.355</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>1.326</td>
<td>1.195</td>
<td>1.207</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prior ID Theft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.608 **</td>
<td>0.589 **</td>
<td>0.579 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know Anything About Offender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.709</td>
<td>0.592</td>
<td>0.621</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know How Information Obtained</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>1.223</td>
<td>1.075</td>
<td>1.094</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Length of Time Information Misused</td>
<td>1.345 ***</td>
<td>1.171 **</td>
<td>1.161 *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Made Aware by Financial Institution</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>1.065</td>
<td>1.151</td>
<td>1.155</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reported to Law Enforcement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>6.058 ***</td>
<td>4.244 ***</td>
<td>4.253 ***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reported to Financial Institutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Yes</td>
<td>0.657</td>
<td>0.676</td>
<td>0.660</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Income</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Female</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Black</td>
<td>2.331 ***</td>
<td>1.816 **</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>1.064</td>
<td>0.997</td>
<td>0.968</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marital Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmarried</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Married</td>
<td>1.041</td>
<td>1.046</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Region</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeast</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Midwest</td>
<td>0.817</td>
<td>0.794</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>South</td>
<td>0.749</td>
<td>0.697</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>West</td>
<td>0.839</td>
<td>0.872</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pseudo R²</td>
<td>0.072</td>
<td>0.076</td>
<td>0.109</td>
<td>0.011</td>
<td>0.115</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001
as in Model 2, although some effects decreased with the inclusion of measures of seriousness, including reporting to law enforcement. Further, the length of time one’s information was misused was less significant in this model ($p \leq 0.01$). Interestingly, when controlling for situational variables in Model 3, suffering an out-of-pocket loss was not a significant predictor of reporting to credit bureaus. The effects and significance of the time spent resolving the incident and distress were similar in Model 3 to Model 1, however the significance of the amount taken was reduced ($p \leq 0.05$).

The estimates in Model 4 present the effects of sociodemographic variables on reporting to credit bureaus. Race/ethnicity was the only significant variable: individuals identifying as Black were over twice as likely to report to credit bureaus than those identifying as white ($p \leq 0.001$).

Model 5 presents the full model, with estimates displaying the impact of measures of seriousness on reporting to credit bureaus when controlling for both situational and sociodemographic variables. The direction and significance of the measures of seriousness remained the same as Model 3. Similarly, situational variables were similar in Model 5 to Model 3, although the significance of the length of time one’s information was misused on reporting to credit bureaus was reduced ($p \leq 0.05$). The effects of sociodemographic variables were similar in Model 5 to Model 4. Respondents identifying as Black had an increased likelihood of reporting to credit bureaus compared to those identifying as white ($p \leq 0.01$), although the race/ethnicity variable was no longer significant overall.

In Table 6-8, Models 6, 7, and 8 estimated interaction effects between out-of-pocket losses and the other measures of seriousness when reporting to credit bureaus. The interaction
effects between out-of-pocket loss and the amount taken (Model 6) and the time spent resolving the incident (Model 7) were statistically significant, although the interaction effect with distress was not (Model 8).

Table 6-8: Logistic regression predicting identity theft victims reporting to credit bureaus (n = 5,753)

<table>
<thead>
<tr>
<th></th>
<th>Model 6</th>
<th>Model 7</th>
<th>Model 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Pocket Loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>7.871 **</td>
<td>3.832 **</td>
<td>1.657</td>
</tr>
<tr>
<td>Amount Taken (log)</td>
<td>1.171 **</td>
<td>1.124 **</td>
<td>1.117 *</td>
</tr>
<tr>
<td>Time</td>
<td>1.376</td>
<td>1.458 ***</td>
<td>1.353 ***</td>
</tr>
<tr>
<td>Distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mild</td>
<td>0.777</td>
<td>0.760</td>
<td>0.722</td>
</tr>
<tr>
<td>Moderate</td>
<td>1.339</td>
<td>1.310</td>
<td>1.468</td>
</tr>
<tr>
<td>Severe</td>
<td>1.255</td>
<td>1.197</td>
<td>1.452</td>
</tr>
<tr>
<td>Out-of-Pocket Loss*Amount Taken (log)</td>
<td>0.717 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out-of-Pocket Loss * Time Spent</td>
<td>0.675 **</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out-of-Pocket Loss * Distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Not at All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Mild</td>
<td></td>
<td></td>
<td>1.599</td>
</tr>
<tr>
<td>*Moderate</td>
<td></td>
<td></td>
<td>0.442</td>
</tr>
<tr>
<td>*Severe</td>
<td></td>
<td></td>
<td>0.394</td>
</tr>
<tr>
<td>Pseudo R²</td>
<td>0.120</td>
<td>0.120</td>
<td>0.120</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001
Each model controlled for all situational and sociodemographic variables tested above. For the complete table with control variables, see Appendix F.

The data in Model 6 reveal that out-of-pocket loss was related to a nearly eight times increase in reporting to credit bureaus ($p \leq 0.01$), and each logged unit increase in the amount taken increased the likelihood of reporting by nearly 1.2 times ($p \leq 0.01$). However, the interaction effect produced an odds ratio of less than one ($p \leq 0.01$), indicating that for those who suffered out-of-pocket loss, each one-unit increase in the logged amount taken related to a decreased likelihood of reporting. This relationship is displayed in Figure 6-2, where predicted probabilities of reporting to credit bureaus are presented while holding all other variables constant at their means or proportions. Here, for those who recuperated losses, their predicted
probability of reporting to credit bureaus increased from less than 0.03 at the lowest amount taken to 0.09 at the highest amount taken. In contrast, for those who experienced out-of-pocket loss, their predicted probability of reporting declined from 0.13 at the lowest amount taken to 0.04 at the highest amount taken.

![Figure 6-2: Predicted probabilities of reporting to credit bureaus based on amount taken for those suffering out-of-pocket losses and those recuperating losses](image)

The estimates in Model 7 display a similar interaction effect between out-of-pocket loss and the time spent resolving the incident. Experiencing out-of-pocket loss predicted an almost four times increase in the likelihood of reporting to credit bureaus \( (p \leq 0.01) \), while each one-unit increase in the time spent resolving the incident increased the likelihood of reporting by 1.5 times \( (p \leq 0.001) \). The interaction effect once again represents a decreased likelihood of reporting to credit bureaus \( (p \leq 0.01) \), where the effect of time spent resolving the incident was less impactful for those who suffered out-of-pocket losses than those who recuperated losses. Figure 6-3 displays the predicted probabilities of reporting to credit bureaus at different times for those who did and did not suffer out-of-pocket losses, holding all other variables at their means.
or proportions. Once again, for those who recuperated losses, greater time spent resolving the incident related to an increased likelihood of reporting to credit bureaus, from 0.036 at less than a day to over 0.10 at three months, six months, and a year or more. However, for those who suffered out-of-pocket loss, their predicted probabilities remained relatively stable across time spent resolving the incident, decreasing slightly from 0.085 at less than a day to 0.078 at a year or more.

![Figure 6-3: Predicted probabilities of reporting to credit bureaus based on time spent resolving incidents for those suffering out-of-pocket losses and those recuperating losses](image)

**Figure 6-3:** Predicted probabilities of reporting to credit bureaus based on time spent resolving incidents for those suffering out-of-pocket losses and those recuperating losses

### 6.2.5 Summary

In sum, quantitative analyses of the representative American sample reveal that most victims of identity theft who had money, credit, or goods taken reported to financial institutions (95 percent), while fewer than one in ten reported to law enforcement and credit bureaus (6 percent each). Further, reporting to law enforcement predicted an increased likelihood of reporting to credit bureaus, and vice versa. These findings provide insight into the predicted
reporting trends of victims based on the consequences and situational characteristics of identity theft incidents.

When examining measures of seriousness, having greater amounts taken increased the likelihood of reporting to law enforcement and credit bureaus, but did not significantly predict reporting to financial institutions. Similarly, greater time spent resolving identity theft related to increased reporting to law enforcement and credit bureaus but not reporting to financial institutions. Having experienced mild, moderate, or severe distress increased the likelihood of reporting to police and financial institutions when compared to those who reported no distress, but these categories were not significantly different from the reference category for reporting to credit bureaus.

Further, experiencing an out-of-pocket loss increased the likelihood of having reported to police and decreased the likelihood of having reported to financial institutions. Suffering out-of-pocket loss did not increase the likelihood of reporting to credit bureaus when controlling for other variables. However, when interaction effects were calculated between out-of-pocket loss and other measures of seriousness, out-of-pocket loss increased the likelihood of reporting to credit bureaus. The interaction effects suggest that the amount taken and the time spent resolving the incident were less impactful upon reporting for those who suffered out-of-pocket losses compared to those who recuperated losses. Similarly, increased time spent resolving the incident impacted police reporting less for individuals who experienced out-of-pocket losses than for those who recovered losses.

In terms of situational variables, having previously experienced an identity theft incident decreased the likelihood of reporting to credit bureaus. Knowing how one’s information was
obtained increased the likelihood of reporting to police, while having knowledge about the offender increased the likelihood of reporting to police but decreased the likelihood of reporting to financial institutions. Finally, being made aware of the incident by a financial institution predicted increased rates of reporting to financial institutions but a decreased likelihood of reporting to police.

Taken together, the findings suggest that measures of seriousness generally lead to increased rates of reporting to law enforcement and credit bureaus. These trends are important for understanding which incidents are reported to particular institutions, including which types of victimization are more likely to be captured in law enforcement statistics.

### 6.3 Qualitative Reasoning for Reporting to Institutions

In addition to the trends in reporting identified based on the American sample, interviews provided an excellent opportunity to further interrogate the reasons for reporting and not reporting to institutions. I argue that victims’ framings of incidents connect to their understanding of the problems’ practical solutions, thereby influencing their reporting decisions. Many participants chose to first report to the institution where their accounts or identity were misused or compromised, and often only pursued further actions when the initial institution was unable to solve the problem. Moreover, victims’ reporting decisions related to the advice they received from loved ones and institutional actors along with their emotional reactions following identity theft.

#### 6.3.1 How Framing Informs Reporting & Perception of a Reporting Hierarchy

The previous chapter discussed how participants framed incidents in numerous ways, including as crimes, inconveniences, institutional failures, and relational issues. Based on these
understandings, participants tended to report in ways they viewed as practical to resolve the issues they experienced. For example, participants who understood incidents as inevitable, inconvenient, or only technically criminal did not report to police, often citing that they did not face significant repercussions. The only participants who reported to law enforcement, Dalton and Winston, understood the events they experienced as criminal.39

Overall, those who viewed incidents as inevitable inconveniences or only technically criminal first contacted the institution where accounts were compromised or where charges were placed. They seldom contacted secondary institutions such as credit bureaus, and usually only did so when the incident remained unresolved or when someone recommended that they report it further. Moreover, those victims who were notified by their financial institution did not contact police, which is similar to the finding in the American sample that being made aware of the incident by one’s financial institution decreased police reporting.

When victims experienced the misuse of one or two specific accounts, including a bank account, credit card, or account with a retailer, they usually contacted that institution first and only sought further support if the company or financial institution could not reimburse losses or resolve the issue. For example, Phoebe, whose credit card was misused online, said she did not act further after contacting the bank because: “I felt like it was resolved.” Regan, in discussing her reporting decisions, simply stated: “I knew that [my wireless provider] and Paypal would be able to handle it.”

39 In Winston’s case, he reported to police when he understood the misuse of his tax information to be criminal. Later, he came to understand the issue as an institutional error.
It was often only when participants perceived that companies were unable to handle the incident that they reported to other institutions. For example, Grant’s credit card information was misused in the United States through a food delivery company. He expected that the company should have been able to identify the charges as suspicious since they followed a password reset, originated internationally, and totalled over $900 in only two transactions from restaurants. Grant explained to me that he called the company and that “they told me that there was nothing that they could do, but they did open a ticket and launch an investigation. I said like, ‘I want my money back right now!’… and they said, ‘Well, we can’t do that’ [laughs].” Because he was uncertain of how long the investigation would take and was frustrated that he would not be reimbursed immediately, Grant called his credit card company, who refunded some of the money up front and the rest after the investigation was complete. The credit card company eventually reimbursed interest charges as well. This demonstrates how some victims will go to additional institutions only when they perceive that the first one has failed to meet their needs.

Like Grant, some participants whose credit cards were misused through another company contacted that company first, then their financial institution when interest charges resulted from the fraudulent charge. For example, Edward accrued interest charges on his credit card while Amazon investigated fraudulent charges. After being reimbursed by Amazon, Edward called his bank to see if they could reverse the interest:

I realized I was going to get charged interest. But I didn't contact them at all at the beginning, which was… kind of like stupid, but at the same time, I guess I was thinking it’s all Amazon right? Like they are the one who has to fix it. If I called [the bank], I'm pretty sure they would say the same thing: ‘Contact Amazon.’

From these examples, it is apparent that most victims took practical approaches to recuperating losses, reporting to the institutions perceived as necessary in order to get their money back.
Few participants reported to credit bureaus. Those who did included Winston, who reported as a precaution since he thought someone had obtained his social insurance number, and Courtney and Dalton, who each had credit products opened in their name and were advised to contact credit bureaus by their financial institutions. Courtney had many credit products opened fraudulently, which began with her receiving new credit cards in her mailbox. Thus, she began calling the issuers one-by-one. Courtney described the process of her experience:

I phoned a couple of them, and they said, ‘Well, yeah, you called on this day and you applied for this and…’ I was like ‘No, I didn't do that…’ I can't remember which bank or credit card company it was, but one of them was really helpful and they said, ‘Okay, here’s what it sounds like has happened, and here’s what you need to do.’ And that's where I found out about, you know, contacting the credit agencies and getting your reports… by the time I got the report from the credit agency, it was like, I can't remember, 10 or 15 different things that had been applied for…that was definitely not me.

Courtney attributed her decision to contact the credit bureau to the financial institution’s recommendation. Contacting the credit bureau also saved her time over calling the financial institutions one-by-one and revealed to her the true scope of the incident. In contrast, many participants expressed that they had not thought to report to credit bureaus. For example, Jake stated: “Honestly, it hadn't crossed my mind. It may have if it was like a huge amount of money, but you know.” Overall, these examples illustrate that many participants reported to the institutions that they perceived as being most easily able to reimburse losses and secure their accounts.

6.3.1.1 Institutional Failures

Participants who framed incidents as institutional failures were more likely to avoid a specific company or institution moving forward. In some cases, avoiding an institution served as an alternative method of resolving incidents. To these participants, this was perceived as a
practical solution to avoid further security issues. Although some other participants, like Grant, opted to stop using particular companies after negative experiences with their customer service, those framing incidents as institutional failures stopped using companies due to the incident itself rather than the institutional responses.

Edward described that the gas station chain where his loyalty points were misused had a location he regularly filled at for work. After the incident, which he researched and understood as a widespread company security issue, Edward said: “I simply stopped filling gas there. Even though it was literally down the street, like less than a minute for me… I would go out of my way to fill other places.” Similarly, after receiving notice that her health information was misused by an employee, Sydney did not opt to report the case to law enforcement or contact the institution itself; instead, she chose to avoid the healthcare institution altogether, going elsewhere for future needs. Finally, after Ian’s father misused his bank account, he understood the issue as resulting from a particular bank branch’s security failure because employees knew Ian’s father well. Although he reported to the bank prior to realizing it was his father, Ian explained that: “…after a few weeks I still noticed that he was doing this, and so I had to completely shut down this account and open up a new account at a different bank.” When participants understood the incident to have resulted from security failures at institutions, they often saw it as practical to avoid that company or institution after resolving, or in order to resolve, the incident.

6.3.1.2 Relational Issues

Participants who viewed the incidents as relational issues also had different understandings of what the appropriate actions were to resolve it. Ian, Chandler, and Benjamin framed their misused accounts as relational issues and all three were selective in reporting and
discussing their incidents with others. Ian was the only one of the three who reported the incident to his bank, and he initially did so when he thought the perpetrator was a stranger. Rather than report the misuse of their accounts to financial institutions, Benjamin and Chandler both changed their accounts’ passwords and PINs without disclosing the reason for doing so to the bank employees. In turn, both attempted to recuperate losses by discussing the issues with the perpetrator.

Benjamin expressed that he discussed the misuse of his accounts with his father, but that “it was never, like, resolved.” When I asked whether he reported the incident elsewhere, Benjamin replied: “I mean there wasn't much I felt like I could do, right? Because…even if I did do that, I would be taking money away from my own family.” At the time that I spoke to him, Benjamin had not yet been reimbursed and did not hold out hope that he ever would be.

Chandler was repaid by her mother but was not sure how much was originally taken and if that corresponded to the amount repaid: “I mean she paid me back. Whatever, I don't know how much of what she actually took, she paid back.” Similar to Benjamin, Chandler expressed that she did not think it was appropriate to report the incident elsewhere: “Within my family, there's always been like a strong sense of resolving inter-familial disputes inter-familiarily.” All three participants said that they would not report a family member to police for the misuse of their account. Moreover, these participants were less likely to disclose the incident to others generally: both Benjamin and Ian had only ever discussed their incidents with siblings.

The framing of incidents – as criminal events, inconveniences, institutional failures, or relational issues – can therefore relate to how individuals act following victimization. While participants who framed the incidents as minor inconveniences or inevitable were more likely to
report to companies or financial institutions but not to police, those framing incidents as relational issues were less likely to report incidents at all. Finally, those who understood incidents as institutional failures or breaches were more likely to close their accounts or avoid that institution rather than formally report the incident.

6.3.2 Advice and Support in the Aftermath

Although many victims reported in ways they viewed as practical based on their understanding of the incident, some participants also followed advice received in the aftermath. This is clear in Courtney’s case, as she contacted a credit bureau following the advice of a credit issuer. Similarly, other participants’ reporting decisions were informed by advice from both institutional actors and others, including family members.

Participants who disclosed the incidents to family members often followed the advice they received. Logan explained that when he first noticed credit card fraud on his account, he contacted his mother, who had experienced a prior victimization, and took her advice: “I spoke to my mom; she had a similar thing that happened to her and they gave her the money back.” At her recommendation, Logan called the bank who launched an investigation and suggested no further actions on Logan’s part. Similarly, Hunter told their parents about their experiences with credit card fraud and added: “They were obviously like, ‘Yep, like, call the bank right away and figure out what was happening.’” Kathryn, who was notified by her credit card company about a suspicious transaction on her account, expressed that she first “just called the bank back and I kind of assumed that they would be taking care of it.” She then mentioned it to her father, who had knowledge about the steps to take following victimization because of his profession, which influenced her decision to not report further:
I think probably if that wasn’t his profession, and he didn’t know that much about it, I would have looked into it a bit further…but I sort of like ran it by him, and then I just left it at that point.

Similar to Kathryn’s experiences, results from the American sample revealed that victims who became aware of an incident after being contacted by a financial institution were more likely to report to the financial institution but less likely to report to police. As Phoebe explained,

I was in exams, and that was the first time it ever happened to me… So I wasn’t completely sure what I was supposed to do. So, I just called them and they just ran through everything for me.

After the bank began their investigation, they left the impression that they would resolve the incident, so Phoebe did not report further. Other participants who reported to banks or credit card companies where employees recommended no further action were likely to not report further. For example, Hunter reported to a bank because their credit card was misused, but Hunter’s personal information had also been compromised through a phishing attack. I asked if the bank suggested contacting a credit bureau or the police, and Hunter replied that “They [did] not mention anything like that.” Dalton was also victim to a phishing attack and had a new account opened in his name. Unlike Hunter, Dalton reported to a credit bureau because his bank recommended it due to the possibility of other accounts being created or compromised. These examples illustrate that victims frequently followed the advice of family members as well as the advice provided by financial institution employees when making reporting decisions.

6.3.3 Emotional Reactions

In some cases, reporting decisions related to participants’ emotional reactions following identity theft. The previous chapter described how many participants experienced initial panic over the uncertainty of having an account compromised. Victims experiencing panic were also
likely to contact the financial institution or company where the account was compromised, although they often did so more urgently. Marshall described receiving a message indicating that his phone provider obtained a request to port out his phone and to call an attached 1-800 number if he did not authorize it. He initially thought that the message itself could have been spam, and he immediately searched online. Quickly skimming the results, he found the story of another victim who received the same message prior to having their phone fraudulently transferred to a different carrier. Marshall expressed:

I was reading it and it was, it was telling about someone who received this message and then had their number ported out to a different company… as a result of something, you know, unscrupulous means like a fraudulent transaction. So, at this point, that’s when my heart rate went to like 180 beats…it was like BRRRRR, it was bumping out of my chest and I got really, really, like, nervous, so I was like ‘Oh my god, like, you know, it seems like someone’s trying to take over my cell phone number’… So the first thing I did immediately then was I called that number and it turns out it, it was a [company] number.

Marshall described that once he realized the message received was legitimate, he panicked and reacted by contacting the company quickly. Similarly, Edward was able to watch as items were added to his Amazon cart and was already panicked and looking for Amazon’s contact information:

I had to find a phone number and calling them letting them know what happened and then within that 10 minutes, the guy ordered all those items… Yeah, and he literally put his own address into my address book… and he literally had all these items shipped to him. So, then I'm literally freaking out.

The reaction of immediately calling the company where the account was compromised was common in instances where participants expressed fear over potential repercussions. This may tie to the finding from the American sample that participants experiencing severe distress were more likely to have reported to each of the institutions.
6.3.3.1 Self-Blame, Embarrassment, and Selective Disclosure

Participants’ anticipated reactions from institutions and individuals also informed their reporting and interactions following victimization. Several participants expressed role-taking emotions, including embarrassment, which impacted how and to whom participants disclosed incidents. In some cases, embarrassment arose from comparisons between the self and common perceptions of victims as naïve.

First, some participants were selective with disclosing incidents to parents, who may have afforded advice on steps to pursue. Amanda, in describing the takeover of a social media account, expressed that: “I think I talked with my friends mostly because I know that, like, my mom would just not take it seriously [laughs]. So, yeah, it was like mostly my friends.” Similarly, Nolan was embarrassed that he had his credit card stolen and misused at a bar. He said: “I didn’t want to talk to my mom, because she’d be like, ‘You’re an idiot,’ [laughs], like she wouldn’t be like mad at me, but she’d be like, ‘That’s disappointing.’” These examples illustrate that participants were selective when disclosing incidents to others.

Moreover, anticipated reactions from institutional actors can impact reporting decisions. Nolan expressed that: “I didn’t like report it right away, because I was like, ‘Okay like, I don’t know how it’s going to look.’” Later in the interview, Nolan added that:

I kind of called in feeling like a little embarrassed, like oh, this is kind of embarrassing, like I’m a student, like, ‘Oh, my money got spent at a bar, I don’t know if they’re going to take me seriously’ kind of thing.

Phoebe also anticipated negative reactions when reporting the incident to her financial institution. She stated: “They didn’t like, judge me about it, like, ‘Oh my god, another young girl using her credit card wrongly, gets fraud on her account.’” In these two cases, Nolan and Phoebe
eventually reported and recuperated their losses. Nonetheless, they both anticipated negative reactions, which could impede help seeking for some victims.

To summarize, a number of factors played a role in interview participants’ reporting decisions following an identity theft incident. First, participants’ framings often influenced the actions they saw as suitable and practical for resolving the incident. Participants were most likely to contact the institution where their identity or account was misused or compromised. Often, only if that institution failed to secure their account or reimburse them promptly did participants report to other institutions. Moreover, advice received from others and emotional reactions influenced the participants’ reporting decisions and actions in the aftermath of identity theft.

6.4 “No Harm, No Foul”: Reasons for Not Reporting to Police

Overall, only two participants reported incidents to police: Dalton, because it was recommended by the bank after a new line of credit was opened in his name, and Winston, who reported the misused tax filings to many institutions before eventually finding a tax center that could resolve it. The remaining participants expressed many reasons for not reporting to police. As mentioned, those victimized by family members generally did not report to institutions and all expressed that they would not report their parents to police. Further, many participants stated that they did not report to police because they resolved it another way or because the incident was not serious enough to report. Finally, some participants expressed that they did not know what reporting to police would accomplish, they were unsure what to do, or that reporting to police would create more work.
6.4.1 The Incident Was Resolved Another Way

The most common response from those who did not report to police was that they felt they had resolved the incident another way without experiencing significant harm. This follows the theme of victims’ reporting incidents in manners they viewed as practical and only pursuing further action when incidents were not resolved through the first institution contacted. Several participants expressed that because banks or credit card companies reimbursed the fraudulent charges, they felt that no further action was required.

Hunter and Phoebe each reported to financial institutions and mentioned that the employees they talked to recommended no further actions. Hunter expressed:

I think because of the fact that the bank did resolve all the charges that were fraudulent, like I didn’t feel it was necessary to contact the police, because I felt that, I guess, the institution in themselves had taken care of the matter.

Similarly, Phoebe expressed that her reason for not reporting to police was that she had already been refunded:

I feel like police wouldn’t really do anything that would help me…because the credit card company already refunded me my purchase and got me a new credit card, so I didn’t really need anything else.

Because Hunter and Phoebe did not feel they needed additional help beyond being reimbursed, they both chose not to report further.

Similarly, when Nolan’s credit card was stolen and misused, he also expressed that he chose to report only in order to be reimbursed. Nolan stated:

I just kind of called the bank. I didn’t really… use the jump of like calling like police, calling like a credit bureau or anything like that, because I was like ‘I don’t really know where it’s going to go from here,’ I kind of was taking it one step at a time. And then when the resolution came that like the charges were disputed and like it all came back to my account, I was like ‘You know what, like honestly… no harm no foul kind of thing.’
These participants’ reasons for not reporting to police illustrate that victims who recuperated losses often felt no further action was required. This parallels the findings from the American sample that out-of-pocket loss increased police reporting.

6.4.2 "RCMP is like a Big Deal”: The Incident Was Not Seen as Sufficiently Serious for Police

As discussed, the way participants framed the incident impacted their decisions to report to various institutions. Moreover, the previous chapter discussed how several participants compared their experience to common cultural depictions of identity theft that they perceived as more serious. Similarly, some participants expressed that they did not report to police because the incident was not sufficiently serious, suggesting that they saw an incompatibility between their understanding of the incident and other incidents that would be suitable for police response.

Courtney, who experienced the creation of many credit products in her name, downplayed the incident relative to other crimes, including Ponzi schemes. With respect to police reporting, Courtney said she did not report because:

The police they just made it seem like if I phoned them, it was a really big deal. And to me it didn't seem like a massive deal. It was irritating and I felt kind of like, you know, somewhat violated, but it just didn't feel like I need to call the police about this.

From this, it is apparent that Courtney’s perception of law enforcement’s role did not align with responding to cases of new account fraud. In Kathryn’s case of credit card fraud, she also compared the incident to related crimes she perceived as more serious. When asked why she did not report to police, Kathryn expressed:

…because it was just specific to my credit card, the number being used, right? Like just the credit card, not my social insurance number or something that could be applied across different sort of sections of my life and my credit.
Kathryn reported perceiving credit card fraud as a routine inconvenience and felt that it would only be suitable to contact law enforcement in more serious instances of identity theft.

Similarly, Amanda, who framed the misuse of her social media as trolling, also expressed that her incident was not sufficiently serious to report to police and described the type of incident she would expect to report: “I feel like, you only escalate that situation when it’s very serious, like stalking or, you know, they get other information through your account, like… money, you know.” Participants comparing the incident to other crimes felt that reporting to police was incompatible with their understanding of the events they experienced.

Finally, Nolan did not report the misuse of his credit card to police because he recuperated the losses, and he also described a previous incident where he thought reporting to law enforcement seemed unsuitable for scams. Nolan told me that he had once ordered a coat online and after sending the money, he never received a shipping label. Nolan was surprised when he called Canada Post and they suggested he contact the RCMP:

I called Canada Post, and they’re like, ‘Oh you need to open up a ticket with RCMP.’ And I was like ‘Is that like actually what I need to do?’ [laughs]… like I feel like that’s super serious… But I like thought that was so crazy that like RCMP had to do that, because I’m like RCMP is like a big deal, not like, um, call because someone’s going to take a coat from you, that sort of thing, so I was like ‘Holy smokes,’ like, I couldn’t believe that.

Although Nolan eventually resolved the incident without contacting the RCMP, this example illustrates how some victims did not understand identity theft and other scams to be the responsibility of police. Overall, some victims saw identity theft as insufficiently serious to report and, instead, understood reporting to police as suitable for more serious crimes.
6.4.3 Unsure of Practicality of Reporting

Several participants expressed feeling skeptical about the practicality of reporting to law enforcement. First, some felt that the police could not feasibly investigate the incidents based on the information available. Second, some participants had prior experience with police that suggested they would be unwilling to investigate this type of incident.

Participants were often pessimistic (or, realistic) about the amount of resources police would enact to catch perpetrators of identity theft, such that they often did not report to law enforcement if the perpetrator was outside of Canada or if they did not have much information to provide to police. For example, I asked Logan, whose card was misused in the United States, why he did not report to police, and he replied: “Like it just didn’t seem to me that it was anything [in] Canada or anything really… physically related to my location.” Grant provided similar reasoning concerning the misuse of his food delivery account, stating:

* I also would doubt that the [local] police in my area would really care enough to send a report to [the United States] for [them] to go and do a follow-up visit at someone’s house, like, I don’t think the system is that well-lubricated… to be able to actually respond adequately to these kinds of complaints.

These participants expected that police resources would not be spent pursuing perpetrators internationally and thus cited impracticality as a reason for not reporting.

Moreover, some participants who were victimized by perpetrators geographically close to them still felt that they had inadequate information to provide police to make it worth reporting. For example, Courtney speculated that the creation of new credit products in her name resulted from someone dumpster diving for her personal information from her garbage or recycling. Because that still did not point to a specific potential perpetrator, Courtney said:
I think, part of me was also thinking like how in the world would they even catch who did this? Like, what’s the point? Like if I can’t phone them and give them any information, they’re going to be asking me questions like ‘I don’t know how this happened.’ I don’t have like a camera out front, I’ve got nothing. So what are they even going to do, right?

Similarly, Jake’s card was physically taken and misused nearby to the area he worked. He expressed: “Honestly it didn’t seem worth their time… I have no idea how they were going to trace the person anyway.” Thus, several participants did not report because they doubted that the police would be able to adequately respond based on the information available about the incident and perpetrator.

6.4.3.1 Police Disinterested

Moreover, some participants thought reporting was impractical due to personal or relayed past experiences with police. Sydney compared her experience with her misused medical information to a credit card fraud her mother experienced. When explaining why she chose not to report to police, Sydney said:

In the past, my Mom has like reported identity theft to them, and they’ve said like there’s people out there that have lost like millions of dollars, and they’re more focused on those cases. So, to me, it was like, okay there was no financial impact on myself, but I don’t know if they would just tell me to-, like, redirect me back to the [medical institution] or like, tell me to just go to court, sue them or something like that.

Similarly, Grant had previously reported scams to law enforcement through an online reporting system, which led him to believe that the police had no interest in knowing about fraud incidents. Grant stated:

Well, I sort of feel like the police slash RCMP are sort of useless when it comes to cases of fraud… I feel like they don’t respond well in the best circumstances. I have, for instance, reported lots of like scams, phone scams, pretend vacations that I’ve won, that are coming from like numbers in my area, when really it’s somebody, you know, far away at a telephone center… I’ve reported lots of that to, there’s like an
online reporting system…and most of the directions on the online reporting system say like, ‘Please, do not report about these scams, because we already know that they’re happening.’ So, they just seem very disengaged in terms of actually trying to do something concrete, like they didn’t even want the information to begin with.

These examples illustrate that having reported to police in the past, or knowing someone who had, may decrease the likelihood of reporting in the future due to the perception that police do not care to respond to scams and fraud. Overall, some participants did not see reporting to police as practical because the police either could not or would not pursue actions to find the perpetrator or protect future potential victims.

6.4.4 Not Sure What to Do & Lack of Awareness

Some participants expressed that they did not report to police because they were not sure what to do in the aftermath or they lacked knowledge about what police would do to respond.

Tied to the feeling that reporting to police was impractical, Sydney expressed:

I feel like a big reason why I didn’t [report to police] and stuff was because I had like, lack of knowledge about, like, what exactly I should be doing. Um, what the police would do about it and stuff, and if there was even like a case behind that and stuff. Like what would, like… what would me reporting it do exactly?

Similarly, Hunter was reimbursed but expressed that they were unsure if other steps should have been pursued:

Um, so, I kind of didn’t take it to any other steps, like I don’t know to what level, if you are supposed to contact the police or the RCMP or other things like that, and I still actually don’t, so I don’t know other than outside of the credit card company, like, what you’re supposed to do… but maybe that is because in the cases that I’ve had, all the charges were resolved that I felt I didn’t need to, whereas if I was actually out money, I definitely would have looked into further steps as to what I can take, um, to recoup some of that.
Hunter’s quote also illustrates the theme that participants who recuperated losses were less likely to report to police. These examples demonstrate that some participants were not sure whether police reporting was expected or beneficial after being victimized.

Finally, Edward discussed a lack of awareness about the Canadian Anti-Fraud Centre specifically. After one of Edward’s incidents, he looked into options for further reporting and came across this center. Edward stated:

I think they need more… recognition in terms of like general society, so people know that they’re supposed to report incidents to them, because I didn’t know. And I didn’t report to them. But… yeah, now I feel like I could have been part of some kind of change, if I did.

At another point during the interview, Edward expressed regret for not reporting to law enforcement. Participants’ knowledge about how to proceed in the aftermath influenced their reporting decisions, and many participants did not know what role law enforcement could play following an identity theft incident.

6.4.5 Reporting Would Create Work

Finally, some participants expressed that a factor influencing their decision to not report to police was that it would create more work. Many victims spent considerable time dealing with institutions when resolving their incidents and preferred not to take additional steps they perceived as being unnecessary. For example, Nolan expressed: “I was like, it’s just not worth it for me, like I don’t know like what, am I going to press charges for this person for $100 and then have to do all this sort of thing.” Edward felt similarly, while also expecting that police would not want to pursue the offender. After dealing with Amazon over approximately twenty phone calls, Edward expressed his reason for not reporting to police: “You know… I honestly just thought they weren’t going to do anything about it. And that it was just going to open more work
for me with zero… I’ll say zero gain…” Finally, Courtney expressed several reasons for not reporting to law enforcement, including that it seemed impractical and that she lacked knowledge about what level of law enforcement to contact. Further, Courtney added:

…and at that point in time, I had a whole list of forms I had to fill out, and a whole list of organizations or companies that I had to call, and I felt like it was more important to do that, to make sure that I didn’t end up owing a ton of money, to get this kind of on the track of getting fixed, rather than calling the police.

Taken together, these quotes illustrate that participants sometimes decided not to report to police because it would create more work. Similar to the American sample, few interview participants reported to police and their reasoning offers insight about why so few incidents come to police attention. To summarize, participants’ reasons for not reporting to police included that they resolved it alternatively or that it was not sufficiently serious for police attention. Further, some participants thought that the police could or would not pursue the case, that reporting would create more work, or that they were not sure what actions to take or what law enforcement would do.

6.5 “It’s Like You’re Screaming into the Void”: Victims’ Reporting Experiences

Although victims’ reporting decisions often related to their perceptions of the incident, participants’ satisfaction with the resolutions facilitated by institutional actors varied significantly. This study’s final research question sought to understand whether victims of identity theft were satisfied with the resolutions facilitated by the institutions contacted. Some participants expressed complete satisfaction with institutions while others were frustrated, confused, angry, or felt unsupported by institutional responses. Moreover, participants’
experiences with institutions varied even when characteristics of incidents were similar. Some of the most common frustrations participants faced were having to talk to several people before finding one who could resolve the incident, having to call institutions repeatedly, or feeling that instructions were unclear about how they should proceed following their victimization. Other participants described disappointment in feeling a lack of closure following investigations or because they felt employees did not care to help or lacked empathy. I will begin by discussing some of the positive experiences prior to discussing each of these issues in turn.

6.5.1 Satisfaction

Participants cited a number of reasons for feeling satisfied with institutions when resolving identity theft, most commonly because companies flagged transactions for them or because they were prompt in resolving the incident. For example, Kathryn was notified by her bank about a suspicious charge on her credit card and expressed gratitude:

I feel very grateful to my bank for flagging it so quickly, and just the fact that they were able to reimburse it since it was only 300 dollars, like, I know for my husband and I, that wouldn’t have been the end of the world or anything like that…but I was just very thankful for how that was handled.

Jake’s wallet was taken after he lost it during a lunch break. Because it was normal for him to use his credit cards in the area where it was misused, he was even more impressed that a credit card company was able to differentiate the transaction as suspicious. Jake stated:

40 Supplemental queries were performed in NVivo to try to identify whether satisfaction with institutions varied based on the type of fraud experienced or its circumstances, with few differences discovered. One identified predictor of satisfaction, described below, is when a credit card company flags a suspicious transaction and contacts the customer. However, it remains unclear what causes credit card companies to flag some transactions as suspicious and not others. The complexity of the cases and number of accounts compromised did not relate to stark differences in satisfaction, with Regan and Courtney both mostly satisfied with institutions while Winston and Dalton were mostly unsatisfied.
I’m not going to lie - I was really impressed by it. Because… I don’t use that card that often and… if I were to look at it in a vacuum, I would think, ‘Oh this purchase seems very random,’ like you know, I might flag it, but for some reason they knew that, you know, either it being the time or whatever, they knew that that one wasn’t legitimate, so… like, I don’t know how they do it, but I was impressed.

Jake had a second credit card misused where the company did not flag the incident and was thus more pleased with the one that had. Participants tended to be satisfied with resolutions when institutions proactively noticed suspicious transactions.

Other participants expressed satisfaction when institutions resolved their incidents promptly. Nolan, who was hesitant to contact his bank for fear of how it would look, was satisfied because the bank employees were kind, but also because they resolved the incident easily. Nolan stated: “The bank was like pretty prompt about it, so it was pretty good.” Peter was similarly impressed with Amazon’s customer service when unauthorized charges appeared on his account, stating:

It was three in the morning, but Amazon customer service works 24/7, so I just gave them a call and issued a complaint and then they just took off the order for me so I didn’t lose any of my money after that.

Finally, Regan’s case was more complex since both her Paypal and phone account were misused. Nonetheless, she was completely satisfied with both companies, saying, “It was so quickly resolved and I was so happy about that.” Further, Regan expressed that both companies “were very, very awesome with that. And I know that some people have had really, really bad experiences with both companies. And I can firmly say that I was not one of them.” When companies resolved incidents promptly, victims were usually satisfied. Unfortunately, many participants’ experiences were not characterized by prompt responses.
6.5.2 Transferring from Department to Department

Some victims felt frustration with institutions when they were referred to multiple departments to resolve incidents. With respect to the multiple institutions that can be involved in fraud’s resolution, Button, Lewis, and Tapley (2009) observed that in the United Kingdom, many victims experience a ‘merry-go-round’ effect, where institutional representatives are disinterested in assisting victims and instead refer them to another institution. In the current study, participants felt similar frustration when they could not find an employee who was interested in helping them and were instead transferred to other departments within an institution, often to fraud departments. For example, Grant expressed:

> When I called [the credit card company] they said ‘Oh, that’s not us that takes care of it, that’s our fraud investigation department and we don’t have their direct number,’ like it was very difficult to actually speak to someone to help me.

Marshall’s phone account was fraudulently transferred out in the evening, which was after the company’s fraud department had closed. He called the number he was instructed to since he did not authorize the port, and he saw the incident as an emergency given his phone account was connected to his banking, other payment systems, social media, and e-mails. Because the message he received had instructed him to call a company number, it was clear to Marshall that any employee could stop the porting request if they had the appropriate knowledge. Nonetheless, when he got through, Marshall expressed: “The person I spoke to… was like, ‘Well, you know what, [pshhh sound] here, call fraud, it’s fraud’s problem, it’s not mine, I can’t do anything to help you.’” Marshall had to contact the company again in the morning.
Ultimately, his phone was ported back by a general customer service representative rather than someone in the company’s fraud department.41

Winston contacted the most institutions of anyone I spoke to, including police, credit bureaus, a lawyer, the CRA, and several tax centers. Winston expressed frustration with how long it took to find anyone willing and able to resolve the false tax filings in his name. Further, he expressed that dealing with the CRA was “the biggest headache,” because nobody he called seemed to have any idea which department could assist him. In describing this frustration, Winston stated:

Just like, the hours involved in originally resolving this was the most frustrating part, because it went on for months. And just those evenings, you know, just getting on a phone line, waiting to get through to the customer service or the customer agent, just for them to say: ‘I have no idea.’ You explain your story again, they give you another number. You call them the next day and it’s just like this cycle over and over and over again.

In cases where victims were referred to other departments, it was common for them to report increased frustration. Moreover, Marshall’s and Winston’s cases illustrate that some employees appeared to not know where to redirect victims, which could lead some victims to remain unassisted.

6.5.3 Hounding for Help & Unmet Timelines

Some participants felt that they had to contact companies or financial institutions excessively before being reimbursed. In many cases, this also related to company employees failing to meet timelines for returning calls or reimbursing victims. Edward, whose computer

41 Interestingly, Regan, who was also victim to a phone porting scam with a different company, had a much better experience, reporting that the representative dealt with the incident promptly while inspiring confidence that it would be resolved.
was compromised while beta-testing software, watched items being added to his Amazon cart before the perpetrator locked him out of his account. After calling Amazon and leaving a message for their fraud department, Edward received a call three hours later explaining that Amazon had frozen and locked his account and that an investigation would be started. The representative said he should expect a call the next business day. After that, Edward said:

From that point on, literally, I was in contact with them probably 20 times and each time I would call in, I would ask him: ‘Did you guys do the investigation? Did you figure out what’s going on?’ And they were like, ‘We just need more time, more time.’ Eventually after probably six, seven weeks, I finally get my money back and I finally get my account back. So, [laughs], it was like the worst month ever.

Edward’s experience was much different than Peter’s, for whom Amazon’s representative simply cancelled the order as soon as he called. In these cases, the time the company took to resolve incidents was central to the victims’ satisfaction. Although something about Edward’s incident may have required more time to investigate, it remains unclear based on the information available to Edward why it took that long.

Grant experienced similar frustration after initially filing a fraud claim with his credit card company:

I think I called them um, around like, two and a half weeks and I said: ‘Hey guys, like I still haven’t got the money back into my account,’ there was a lot of problems with like, getting in touch with the right person, who was doing the investigation.

Grant was eventually reimbursed but never received a call back when promised. Logan’s experience with credit card fraud was similar. Because the charges on Logan’s bank statement were placed in a state he had never visited, he expected that it was clear he had not made the
transaction. After initiating the fraud claim, Logan stated that: “They said they’d get back to me within a week. They didn't.” Later, he explained his frustration with the credit card issuer further:

‘We’ll get back to you within a week.’ A week passed, and they didn't get back to me at all. So, it's just this… it’s disparate time they said to give me feedback, and they didn’t do it. Um, so… that was what I was most upset about.

When corporate employees promised to contact victims and did not reach out to them, it led to frustration. Moreover, some victims like Grant and Edward were left with charges on credit cards for lengthy periods of time, resulting in additional interest charges. Although both were eventually reimbursed by their credit card companies, these employees’ empty promises about timelines contributed to increased financial stress.

6.5.4 Belief That the Process Could Have Been More Straightforward

Related to the difficulties that some victims had finding individuals who could resolve their incidents, several participants expressed that the process of recuperating losses and recovering compromised accounts could have been clearer. Grant, who contacted the food delivery service and his credit card company to launch fraud investigations and recuperate losses, simply said: “I don’t feel like the process was like, as straightforward as it needed to be.” Winston’s case with his misused tax information ultimately led him to report to several different divisions of the CRA and tax centers, the police, credit bureaus, and a lawyer. Winston summarized his experience by saying: “I was not sure what I was to do… I think, yeah, they

\[\text{footnote} 42\]

As noted in a previous footnote and in Jake’s narrative, the specific mechanisms that credit card companies use to flag suspicious transactions are unclear, although it impacts victims’ satisfaction of resolutions of identity theft. International charges were flagged for some participants, yet not for others.
should have a clear way… of helping after someone goes through something like this.” With respect to the CRA in particular, who he spent countless evenings calling, Winston said:

I understand that not everyone in every department is going to know exactly who to direct me to, but I went through dozens and dozens of different people at tax centers and the CRA, and the fact that it took so long for someone to direct me to the right area was frustrating. If that could be where, if anything could be fixed, within realistic terms, I’d love to have a way that other people can report this issue and then have a team help resolve the issue.

Victims sometimes felt that either public institutions or specific company employees could provide clearer instructions on the complete process of resolving an identity theft incident.

Courtney’s case illustrates the multiple ways a victim could resolve new account fraud. Courtney received mail with credit products opened in her name, so she began by calling the companies individually before being advised by one of the employees that it could be more efficient to contact a credit bureau to see all the fraudulently opened products. Sure enough, there were several credit products opened that had not arrived at her door, which she would not have been aware of if not for contacting the credit bureau. Although this employee made the process easier with helpful, time-saving advice, it took Courtney calling multiple credit issuers before hearing this suggestion. This implies that some representatives for credit issuers may struggle to discern the appropriate next steps for victims. Courtney expressed:

I do remember thinking like, ‘Why isn’t there just a thing online, like some kind of resource, where it sort of says steps 1 through 8, here’s what you need to do now.’ You know? Because I kind of had to piece it together.

Later in the interview, Courtney expressed that contacting the credit bureau now seemed like the logical first step, but she added: “Who knows what the actual right first step is. Is there one? I have no idea.” These experiences illustrate that many participants felt the resolution of their
identity theft incident could have been made easier through clearer instructions, either provided online as a public service, or by corporate and government employees specifically.

6.5.5 Lack of Closure

A common theme related to victims’ perceptions of institutional responses was feeling a lack of closure from financial institutions or other companies. This relates to the lack of knowledge many participants had about the nature of the incidents they experienced, including how information or accounts were compromised. Despite Canadian institutions placing responsibility on consumers to protect themselves from identity theft (see Whitston and Haggerty 2008), institutions often reimburse victims but fail to provide them with any information about what occurred.

Logan was unsure whether the misuse of his credit card in the United States was a crime or a simple error. When I asked how the financial institution could have improved their response, Logan expressed that they could have better informed him about what happened:

I mean, I would still like to know why, I think, why it happened. I mean, obviously I assume… it was something on their end and they wouldn’t tell me, but I would like to have some closure. And especially, back when I was using my debit card more… they would freeze it all the time. I guess, you know, people got access to it, or something like that. Um, and I would like to know what happened in those cases too.

When I asked what more he would like closure on, Logan said he wanted “something more concrete as to how or why it happened.” With more information about how the charges occurred, Logan may be better equipped to prevent future unauthorized charges.

Other participants expressed feeling a similar lack of closure. When I spoke to him, Titus had yet to be reimbursed for a fraudulent credit card charge on his account. Further, he expressed that he had been racking his brain as to how the charges occurred. After talking to the bank
employee, Titus stated: “I wouldn’t say I was unhappy, but I mean you’re left hanging.” Grant felt similarly after his experience with his credit card company:

They always told me, ‘Oh I’m going to call you back and give you more information about where we’re at,’ and [I] never got any phone calls and then one day the money just kind of showed up in my account, so I never got any kind of, like, official follow-up from the representative I was speaking to, nobody ever called me to say, ‘Hey we’re putting the money back into your account,’ or to give me the results of their investigation. Like, they just did everything kind of behind closed doors.

These examples illustrate that after interactions with credit card companies or banks, victims sometimes felt confused as to why the institutions did not follow-up or explain the outcome of their internal investigations.

6.5.6 Feeling Unheard & That Employees Did Not Want to Help

Finally, several victims felt that they were unheard throughout the process of resolving incidents. In some cases, this related to the prior frustrations where participants felt that employees referred them elsewhere because of a lack of knowledge or desire to help. Moreover, even in cases where the process was clear, some participants felt employees or institutions were uninterested in hearing about and resolving their issues.

Those dealing with repeatedly calling institutions for support included Winston, Grant, and Marshall. Winston described the lack of understanding he felt when calling different divisions of the CRA. He wished he could talk to someone face-to-face, because: “It was like, you’re calling all these numbers and all that, and then, there’s always that inhuman element of getting, someone on the call center who really doesn’t understand the situation and all that.” Until eventually finding a helpful tax filing center, Winston’s experience was characterized by feeling unheard by actors in various divisions of the CRA.
Grant’s experience with reporting prior scams to police was that they did not want to know about the cases. Moreover, he felt that his experience repeatedly contacting the credit card company only to be reimbursed without knowing the results of the investigation represented a lack of care on the part of the credit card company. Grant described both experiences in one response, beginning with his experience with the online fraud reporting system:

I’ve reported them to the online database, there’s a place that you can report, like, who called you, what is their phone number, etcetera, but the thing that I find quite frustrating with that is that there’s like fifteen steps… and the fourteenth step, says, ‘If this is about winning a pretend vacation, don’t worry, we already know about that one, please don’t submit the report.’ So, it’s like, you’ve already put in all the time to put in, like, the dates, the time, the phone number that called you, whether you were on the phone, whether it was in-person, whether you purchased anything, whether you lost any money, and then on the second last step, they’re like, ‘By the way, we don’t care about this,’ you know? As well, similar to my [credit card] experience, there’s no follow-up, so nobody ever contacts you or sends you a confirmation e-mail, or tries to find out, like, who called you, like what happened, etcetera, or like, ‘We’ve documented your report, thank you for submitting it.’ There’s no, like… it’s like you’re screaming into the void, you know?

When victims did not receive confirmations or contact from the institutions to which they reported, they were likely to feel unheard.

Marshall also had the perception that some employees did not care to help. The unauthorized porting of his phone occurred at night, after the company’s stores and fraud department were closed. Despite this and the fact that Marshall’s phone account could have led to many other payment accounts being compromised, customer service representatives forwarded him to the closed fraud department. Marshall expressed:

I couldn’t go to a store, and you know, nobody really from [the company] wanted to really do a whole heck of a lot to get my number back. Well, you know, Mr. Fraudster has it now, so I’m kind of like, ‘Oh shit’ [laughs].
Because Marshall worked in the telecommunications industry and had researched this type of fraud, he felt he could explain the situation to an employee and knew that it was within their power to lock the account without being referred to a fraud department. Marshall added that the company employees failed to hear him out:

…as long as the person on the phone that I call in is open, and willing, and will listen, and I can explain how to fix it… then we can get it fixed. But some of them are, you know, as you saw, as you heard, right… like, ‘I don’t know what to do, you call fraud, bye.’ You know what I mean, it’s just like…yeah, but they just don’t want to do it, right?

Thus, Marshall’s frustration was not just at being referred to a closed fraud department, but also based on a perception that the representative lacked sympathy and a willingness to listen and help.

In sum, although some participants expressed complete satisfaction with how institutions facilitated the resolution of their identity theft incidents, others felt that the responses or processes could have been improved. While some participants reported frustration with specific institutional actors, most who were disappointed with the resolutions facilitated took issue with the process, including that the steps to resolution were unclear, that timelines went unmet, or that they had to contact several people to resolve the incidents. Even when details of incidents were similar, participants’ satisfaction with the responding institutions varied. For example, while Kathryn was satisfied with the resolution of her credit card fraud, Logan was not; similarly, although Marshall’s experience with regaining his phone number was negative, Regan’s was positive. These differences in victims’ experiences could relate to institutional policies, customer service agents, or some detail of the incident that companies or financial institutions withheld from victims. These possibilities will be addressed further in the discussion.
6.6 Summary

In summary, the present chapter addresses this study’s second and third research questions. Victims tended to take a practical approach to reporting in the aftermath of identity theft with the aim of recuperating losses. As seen in both the NCVS-ITS and the interview samples, victims reported to credit card companies and banks at high rates and reported to credit bureaus and police less often. The quantitative findings suggest that victims who suffered out-of-pocket losses were more likely to have reported to police and less likely to have reported to financial institutions. Other measures of seriousness, including the time spent resolving the incident, distress, and the amount taken, were associated with greater likelihoods of having reported to credit bureaus and police.

The qualitative interview data revealed some additional complexities in reporting decisions. Participants’ reporting was sometimes influenced by their framing of incidents as crimes, inconveniences, or relational or institutional issues. Often, participants were more likely to report to secondary and tertiary institutions only when the first institution failed to reimburse losses. Further, victims were likely to follow advice provided by loved ones and institutional actors, and their reporting decisions could have been influenced by their emotional reactions, including embarrassment, anger, and panic.

Despite identity theft constituting a crime, few victims reported to police. Sometimes, this related to participants’ framing of incidents as minor inconveniences that were issues for institutions rather than law enforcement. Participants who held this view often believed that their incidents were unsuitable for reporting to police in comparison to crimes they perceived as more serious, or they were unaware that their issue was a matter for police. Moreover, some
participants expressed that they did not think the police could or would do anything, or that it would create more work for them.

Finally, this chapter’s closing section argues that victims’ satisfaction with the resolutions facilitated by institutions varied substantially. Some victims reported complete satisfaction with institutions, noting that they were impressed when companies or financial institutions informed them of suspicious transactions or responded to incidents in a timely manner. In contrast, many victims reported frustration with companies, particularly when they needed to contact multiple departments or multiple times, when they felt that the process was unclear, and when they perceived that institutions’ employees were not interested in helping or they felt otherwise unheard. Finally, some participants felt a lack of closure when institutions failed to reveal the results of their investigations, which caused additional frustration. Moreover, not receiving information about how or why an account was misused could cause victims to feel that they were left without potential actions they could take to prevent future identity theft incidents. The next chapter assesses these findings in the context of past research and theory.
7 Discussion

7.1 Introduction

This chapter discusses this study’s findings in the context of past research on identity theft and fraud victims. In Chapter 5, I argued that victim’s understandings of identity theft incidents and the self are processual, with individuals framing incidents in various ways. Moreover, participants often resisted the victim label by downplaying the non-financial harms experienced or by blaming themselves for their role in the incidents. Chapter 6 first presented findings from quantitative analysis of the NCVS – ITS, finding that measures of seriousness increased reporting to police and credit bureaus but had mixed effects on reporting to credit card companies and banks. Specifically, suffering out-of-pocket loss was a strong predictor of reporting to police and credit bureaus, and the results indicate that the other measures of seriousness may impact reporting differently depending on whether victims lose their own money. Moreover, the qualitative analysis revealed that participants’ understandings of incidents informed their views of the incident’s practical solutions and thus influenced their reporting decisions. Finally, while some victims were satisfied with the resolutions facilitated by institutions, many were not and felt that the process could have been more straightforward or that institutional actors were unwilling to help.

In what follows, I discuss how these findings fit within and contribute to past research on identity theft and fraud victimization. This chapter proceeds in the order of the research questions: first examining victims’ understandings of incidents and themselves, then discussing their reporting decisions, and finally assessing their experiences with institutional actors. Connections between the findings are also discussed throughout. The final sections of this
chapter discuss some policy implications of the present study and suggest areas for future research.

7.2 How Individuals Understand Identity Theft and Themselves

7.2.1 The Process of Identity Theft Victimization

In Chapter 5, I argued that identity theft victims’ understandings of incidents should be viewed as processes. This aligns with past research which found that almost three quarters of victims are unsure of how their information was obtained and only six percent know anything about their offender (Harrell 2019:7). Although the experiences of identity theft victims had not been studied previously, Burgard and Schlembach (2013; and Goffman 1952 before them) described fraud victimization as a process characterized by the victim eventually realizing what has occurred. That individuals have varying awareness of what transpired is significant for our understanding of identity theft in society, since most of our knowledge about its prevalence and consequences comes from victimization surveys.

Many victims were initially panicked when they were contacted by companies or when they noticed unexpected transactions, including fearing the extent to which their accounts or personal information were compromised. Some participants learned more details about incidents by checking their transaction histories, while others discovered more information through conversations with the perpetrator or with institutional actors. In fact, some victims felt dissatisfied with institutions when they provided little or no information from internal investigations into the origins of transactions. Accordingly, many victims remained unsure of how transactions were authorized or how their personal information was obtained. Participants
speculated that their information could have been compromised from faulty card readers, breached databases, and even errors made by financial institutions.

Similarly, several participants used internet searches to try to better understand what happened, including searching their own e-mail addresses or the purported company phone numbers who notified them about the incident. This is similar to Cross and Layt’s (2021) finding that victims of romance fraud often searched the internet to try to identify the legitimacy of the potential perpetrator, and this is significant for two reasons. First, it suggests that online resources are likely to be useful if they are accessible through the search terms and platforms that victims use. Second, it indicates that individuals’ understandings of the events before them may be informed by the stories of others found online. For example, Edward’s discovery that multiple users of the same gas station loyalty points program were scammed led him to understand the incident as a company issue. Moreover, Marshall’s search of phone porting scams revealed that many perpetrators use porting to try to access secondary accounts linked to smartphone numbers. While government sources confirm that this is a goal of these scams (see Office of the Privacy Commissioner of Canada 2020), Marshall said that he had monitored all of the accounts attached to his phone and found no attempts to misuse them. Thus, his understanding of the incident and the perpetrator’s intention was partly informed by what he learned online about similar incidents.

7.2.2 Understandings of Identity Theft

In the context of cybercrimes generally, Button et al. (2021) described a continuum of impact through which victimizations are experienced, from minor inconveniences to serious criminal violations. This study’s findings suggest that victims understand incidents that could legally be defined as identity theft within many social frameworks. Not only do victims see these
incidents as crimes or inconvenient events, but also as relational issues, institutional security failures and breaches, clerical errors, and more. This also relates to the processes of victims’ experiences since their understandings often changed substantially when they received new information. For example, where participants’ searches revealed a company had been breached, they often redefined the issues as company security failures rather than as crimes or minor inconveniences.

That victims understand identity theft in several ways demonstrates an apparent routinization of some forms of identity theft. Many participants discussed the expected nature of credit card fraud in modern society, describing incidents as inevitable. Although research has not examined the normalization of identity theft from victims’ viewpoints, several scholars have investigated how messaging surrounding identity theft presents it is a constant threat from which individuals are responsible for protecting themselves (Cole and Pontell 2006; Monahan 2009; Whitson and Haggerty 2008). For example, Whitson and Haggerty (2008) found that government and institutional messaging surrounding identity theft often downplays their responsibility while emphasizing individual actions that can be taken to protect oneself. Monahan (2009) argued that the individual responsibilization of identity theft is just one example of neoliberal approaches to crime and social control in an age where companies and governments hold citizens’ personal information in large, often vulnerable, databases. This downloading of responsibility to the public may relate to the finding that some victims understand identity theft as inevitable or routine.

Moreover, it was unexpected that several participants framed identity theft as a relational issue. While participants victimized by family members were overrepresented in the interview
sample, this framing demonstrates that a subset of victims understand the misuse of their accounts to be a familial issue. These incidents were much less likely to come to the attention of institutions that could reimburse victims; rather, victims often blamed themselves for their role in these incidents and sought reimbursement by negotiating with the perpetrating family member. In Benjamin’s case, that negotiation was unsuccessful, and he was left to pay thousands of dollars out of pocket, resulting in having to take on additional work and stress during his post-secondary career. Although financial victimization of elder family members can be neutralized based on perceptions of an owed future inheritance (see Tomita 1990), scholars have not examined rationalizations and blame when children are victimized. These findings suggest that identity theft involving family members can be hidden from help-seeking institutions.

Participants also varied in how they understood identity theft. While some participants described their incidents as identity theft or fraud, most did not, and some explained that they understood identity theft as something more serious than what they experienced. Scholars like Cole and Pontell (2006) and Monahan (2009) have expressed that the codification of identity theft laws has come to capture several forms of fraud that are not necessarily alike. These findings indicate that some individuals associate identity theft with new account frauds but not misused existing accounts. For example, Kathryn said that her understanding of identity theft was that it only applied to opening new accounts while Amanda laughed at the idea that her misused social media account constituted identity theft, despite someone impersonating and

---

43 One study examined familial identity theft to compare sociodemographic characteristics and forms of identity theft between those victimized by family members and the general NCVS – ITS sample (Navarro and Higgins 2016). However, it did not examine victims’ reporting decisions or experiences.

44 Although the terms “identity theft” and “fraud” were excluded from recruitment materials, these terms were discussed in several interviews.
posting as her.\textsuperscript{45} This demonstrates that identity theft as used in common discussions may not always reflect the forms of fraud included in criminal codes.

This is also significant given that the NCVS – ITS informs much of our knowledge about identity theft in North America. The interview recruitment used the NCVS – ITS inclusion criteria, and interviews revealed that some incidents recorded by the Bureau of Justice Statistics may not reflect incidents that many would consider to be identity theft. While Winston’s tax account was misused without his consent, he had come to believe that it was not a crime committed by a perpetrator but rather a clerical error made by an institution. Similarly, Logan was unsure if his credit card fraud was the result of a crime or an error made by his credit card company. Finally, although Amanda’s social media account was misused by a perpetrator, she understood the incident to be trolling, and researchers may classify this as a form of cyberbullying. In this case, the intent of the perpetrator was unclear, and it is possible that they attempted to access linked accounts even though they ultimately did not. Thus, the inclusion criteria, combined with some victims’ lack of knowledge about the nature of incidents, allowed for ambiguous cases to be included.

\textbf{7.2.3 Criminality and Victim Statuses}

Many participants described understanding incidents as technically crimes and themselves as technically victims. This provides support for past critical contributions to victim research and demonstrates how individuals may afford different privilege to the victim label

\textsuperscript{45} According to the Canadian Criminal Code, Amanda’s case may fit legal definitions for identity theft and fraud depending on the perpetrator’s intent. The perpetrator’s possession of Amanda’s account information, including name, e-mail address, and password, constitutes identity theft if their intention was to commit a crime with that information (C.C.C., RSC 1985, c C-46: s 402.2). Such crimes would include identity fraud, which is misusing someone’s identity information for self-benefit or to disadvantage someone else (C.C.C., RSC, c-46: s 403).
(Rock 2002). However, while victims have been found to identify with the label selectively due to negative associations with the term (Fohring 2018; Leisenring 2006), this study found that victims often resisted the label by rationalizing the harm experienced or by denying that a victimization occurred.

In this sense, the results support past findings on techniques of neutralization and rationalization, suggesting that victims of non-violent crime may rationalize incidents by denying harm or blaming themselves. Scholars have previously extended Ferraro and Johnson’s (1983) domestic violence rationalization techniques to other violent crimes (Tomita 1990; Weiss 2011). Moreover, Copes and Vieraitis (2012) found support for Sykes and Matza’s (1957) techniques of neutralizing offending behaviors in identity theft, finding that many perpetrators denied that they caused harm to victims. In the present study, many participants resisted a victim label by denying that harm occurred when they were reimbursed by financial institutions or other companies. This relates to past presentations of identity theft as a victimless crime, which has been problematized by scholars who describe the lost time and emotional consequences resulting from identity theft (Golladay and Holtfreter 2017; Randa and Reyns 2020). In fact, some of the participants in this study who resisted a victim status by citing the lack of out-of-pocket loss nonetheless reported considerable distress and lengthy times spent resolving incidents.

One way that participants denied the harm they experienced was by comparing themselves to other victims who they perceived as having it worse. Victims often compared themselves to what they saw as typical victims of identity theft, usually individuals who are older and non-technologically savvy. This relates to work by Loseke (2001), who found that some victims of intimate partner violence resisted labels as a victim due to the perception that their
experience did not align with popular characterizations of violence. Moreover, it supports the application of labeling theory to victims of crime, given that Link (1987) and Link et al. (1989) emphasized the importance of prior conceptions in informing whether one will internalize a label.

Similarly, some participants resisted victim labels by blaming themselves for victimizations. Scholars have noted that a victim-blaming discourse surrounds fraud, particularly those forms that involve an active role by victims, such as phishing scams (Button and Cross 2017; Cross 2015). This study found that participants not only self-blamed when they were victim to phishing scams, but also in other forms of identity theft. In turn, this self-blame can be a barrier to victims contacting institutions (see Burgard and Schlembach 2013; Cross 2018b).

7.3 Victims’ Reporting Decisions

To examine victims’ reporting decisions, I analyzed data from the NCVS – ITS and interviews. While the findings must be interpreted contextually, both methods contributed to understandings of victims’ reporting decisions. In North America, the NCVS – ITS is the main source of knowledge about identity theft victims. However, while past research has examined some factors influencing reporting to law enforcement, credit bureaus, and financial institutions (Golladay 2017) and the impact of measures of seriousness on police reporting (Reyns and Randa 2017), no study has examined the effect of measures of seriousness on these three reporting options. Moreover, few qualitative studies have been conducted in North America, and little was previously known about victims’ reasonings for reporting to particular institutions. The findings are first discussed comparatively where they connect and differ, followed by an examination of the unique findings from the quantitative and qualitative analyses.
7.3.1 Similarities Between Samples

Analyses of both data sources revealed that many victims reported to financial institutions, while few reported to law enforcement or credit bureaus. Although this is expected in the context of past research indicating that many institutions may be tasked with responding to cybercrimes (see Nhan 2010), it is nonetheless significant. The assent of Bill S-4 in Canada in 2009 and the criminalization of identity theft in the United States a decade prior (Archer et al. 2012) gave law enforcement the power to charge individuals for identity theft, yet they are made aware of only a small portion of incidents. Scholars have observed the many jurisdictional challenges police may face when responding to online fraud (Cross 2020), and Cole and Pontell (2006) also noted that discourses present law enforcement as helpless in responding to identity theft. Nonetheless, this underreporting implies that few identity theft perpetrators are brought to police attention reactively and that law enforcement, including those tasked with collecting information and preventing identity theft (see Canadian Anti-Fraud Centre 2021), have limited knowledge about its prevalence and nature.

Another similarity between data sources was that victims who knew little about how their information was obtained were unlikely to report to police. The quantitative analysis revealed that knowledge about how one’s information was stolen increased the likelihood that victims reported to police, which was expected based on past research (Golladay 2017; Reyns and Randa 2017). In their discussion of this finding, Reyns and Randa (2017) drew from past sexual

46 As noted, it remains unclear how many identity theft incidents originate online given the reliance on victim surveys to inform knowledge combined with the minimal information that victims have about the nature of their incidents.
victimization literature which found that women are less likely to report to police when they feel that they do not have proof that they were victimized (Fisher et al. 2003). Reyns and Randa (2017) thus posited that victims of identity theft may be more likely to report when they can give police useful information to apprehend the offender. Similarly, in this study’s qualitative findings, some victims expressed that they did not report because they did not see it as practical. This includes Courtney, who suspected her information was taken from her garbage or recycling but had no evidence to present to police that would support this theory. Similarly, Jake expressed that reporting to police did not seem worth the police’s time, adding that he was unsure how they could trace the person who took and misused his credit cards. Moreover, other victims explained that they did not report because of their perceptions that police were unwilling to investigate. These qualitative findings support Reyns and Randa’s (2017) suggestion that knowing how one’s information was obtained increased reporting because of perceptions that police will only investigate identity theft incidents if victims provide sufficient evidence. Overall, this indicates that police are more likely to be made aware of cases where victims can offer some information about the nature of the incident. Whether or not that leads to investigation remains unclear: Australian fraud victims have been frustrated that law enforcement did not investigate cases, including when victims felt they provided actionable information (Cross 2018d).

In this sense, the qualitative findings may contribute to understanding some of the processes behind the quantitative trends. For example, the quantitative analyses revealed that discovering incidents by getting a message or call from ones’ financial institution increased victims’ likelihood of reporting to a financial institution but decreased their likelihood of reporting to police. Through interviews, it became apparent that some victims of identity theft
saw incidents as only technically criminal or as inevitable inconveniences in modern life. In fact, several of those who were notified by their financial institution came to see the incident in this way and often reported only to their financial institution. Moreover, the interview participants generally followed the advice of institutional actors when they were reimbursed, and several took no further action when they received no advice.

The findings from qualitative interviews may thus account for some of the unexplained variance identified in the quantitative analysis. For example, the quantitative analysis could not account for whether victims saw incidents as inevitable and reported only to the company where accounts were misused, or if they viewed the incident as a company security failure and avoided that institution altogether. Moreover, emotional reactions and advice provided by institutional actors influenced interview participants’ reporting decisions, and both factors have been found to inform police reporting for property crimes in the United States (Greenberg and Beach 2004). With similar social contexts surrounding families, company security failures, crimes, and online payment systems, American victims could also understand identity theft in various ways.

7.3.2 Differences Between Samples

Although the samples were similar in their rates of reporting to credit bureaus and law enforcement, their rates of reporting to financial institutions differed, with 95 percent of the American sample doing so but only 65 percent of the interview participants. Along with the differences in sampling between interviews and the NCVS – ITS, this may be partly a product of the inclusion criteria for the quantitative analysis, since variable selection meant that the only victims included had some value of money, goods, services, or credit taken. Moreover, this may also be due to the disproportionate number of interview participants victimized by family
members, with only one reporting to a financial institution. A nationally representative identity theft victim survey of Canadian adults would be necessary to understand whether their financial institution reporting rates differ from Americans.

The quantitative analysis of the NCVS – ITS found that those who knew information about their offender were more likely to report to law enforcement but less likely to report to financial institutions. Although this measure has limited utility for indicating the nature or depth of the relationship, the interview participants who knew their offender were victimized by family members and cited this as a reason for not reporting to police. This likely results from a difference in the samples and those victimized by family members are only one subset of victims who could know their offender.

Finally, the data were conflicting with respect to the effect of distress on reporting to financial institutions. In the quantitative analyses of the American sample, increased self-reported distress related to higher likelihoods of reporting to both police and financial institutions. In interviews, although the victims who contacted police reported high levels of distress, those who reported to financial institutions generally had lower levels of distress. Most victims of credit card fraud that I spoke to experienced only mild distress. Although further research is needed, this may be a product of the lack of causal direction identified in quantitative analysis, since reporting itself could lead to increased distress. Of those who reported to companies, Marshall and Edward both experienced significant distress and each had negative experiences reporting which amplified their negative emotions. Accordingly, the relationship between distress and reporting may be multidirectional.
7.3.3 **Quantitative Findings**

Unique contributions from the quantitative and qualitative samples merit further discussion. The models in this study sought to expand on the past research examining identity theft reporting in North America. While Reyns and Randa (2017) found support for measures of seriousness predicting reporting to police, Golladay (2017) examined reporting to police, financial institutions, and credit bureaus but only incorporated the amount taken as a measure of seriousness. As such, by examining the impact of measures of seriousness on all three of these reporting options, this study provides the most comprehensive tests of relevant measures of seriousness and situational variables on identity theft reporting to date.

Like Reyns and Randa (2017), this study found that the amount taken increased reporting to law enforcement and, similar to Golladay (2017), the amount taken was found to increase reporting to credit bureaus but not to financial institutions. Also like Reyns and Randa (2017), heightened emotional distress increased reporting to law enforcement. Moreover, it was related to increased reporting to financial institutions, although it had no effect on reporting to credit bureaus.

As expected, this study found that suffering out-of-pocket loss increased the likelihood of reporting to law enforcement. Building both on Reyns and Randa’s (2017) finding that out-of-pocket loss was a strong predictor of police reporting and discussions implying that identity theft victims who recuperate losses are a different conceptual group than those suffering out-of-pocket losses (see Koops and Leenes 2006), this study tested interaction effects between out-of-pocket loss and the other measures of seriousness. The findings suggest that the reporting decisions of victims who suffer out-of-pocket losses are less impacted by other measures of seriousness than
the decisions of those who recuperate losses. For example, experiencing severe compared to mild distress and increased time spent resolving incidents impacted police reporting more for those who recuperated losses than those who did not. Similarly, having greater amounts taken and spending longer resolving incidents impacted reporting to credit bureaus more for those who recuperated losses. In the latter case, out-of-pocket loss was not a significant predictor of reporting to credit bureaus prior to testing for interaction effects. This demonstrates the importance of testing for whether these groups’ reporting decisions were differentially impacted by measures of seriousness. Moreover, some relationships were unexpected, including that greater amounts taken decreased the likelihood of reporting to credit bureaus for victims who suffered out-of-pocket loss.

The findings related to out-of-pocket loss are also concerning in the context of past Australian studies finding fraud victims’ cases often go uninvestigated by police (Cross 2018d; Turville et al. 2010) and Canadian findings that identity theft victims have been turned away by police even when suffering out-of-pocket losses (Sproule and Archer 2008). Combined with recent American and Dutch research that those with lower incomes and educational attainment are more likely to suffer out-of-pocket losses (Reynolds 2021; van Wilsem et al. 2021), this suggests that the institutional arrangements of identity theft victim support may best serve the wealthy and highly educated.

Moreover, in the quantitative analysis, suffering out-of-pocket loss was related to a decreased likelihood of reporting to financial institutions. This finding could indicate that victims who did not contact financial institutions missed a crucial step in recuperating losses or that complex cases where victims failed to recuperate losses were more likely to go unreported to
financial institutions. In the qualitative sample, the only two victims that knew\(^{47}\) they paid out of pocket did so because one did not contact any institutions and could not negotiate with the perpetrator and the other’s financial institution would not reimburse the full amount taken. Overall, this suggests that further research is needed on victims who suffer out-of-pocket losses since they may have distinct motivations for reporting or not reporting compared to those who are successful in recuperating losses.

The quantitative results also found support for time spent resolving incidents as a predictor for reporting. Past studies examining identity theft victims’ reporting decisions have not tested the effect of this variable, and this study found that greater time spent resolving identity theft related to increased reporting to law enforcement and credit bureaus. This was expected given that the time spent resolving identity theft can inform perceptions of seriousness (Li et al. 2019) and that some victims can spend months or more resolving incidents (Harrell 2019; Pascoe et al. 2006), which may have secondary consequences including cancelling plans and missing work (Identity Theft Resource Center 2018). While lost time is not often considered as a cost of crime,\(^{48}\) it should not be neglected since it can compound distress and financial costs (e.g., through missed work). The results of the qualitative analyses suggest that the time spent resolving incidents can increase when companies and financial institutions do not assist victims promptly, so some of those reporting to law enforcement and credit bureaus may only be doing so because they feel other institutions have failed them.

\(^{47}\) Chandler was unsure if she was reimbursed for everything taken and Titus had not yet been reimbursed at the time of the interview.

\(^{48}\) For instance, it is not considered in the Canadian Victims Bill of Rights.
Taken together, the findings suggest that measures of seriousness most strongly predict reporting to law enforcement. Not only were the coefficients stronger for reporting to law enforcement, but the variance explained by the measures of seriousness was higher for law enforcement (Pseudo $R^2 = 0.144$) than for credit bureaus (Pseudo $R^2 = 0.072$) or financial institutions (Pseudo $R^2 = 0.040$). This suggests that the few identity theft incidents brought to police attention are often the most serious ones. Results from the qualitative interviews suggested that many victims reported first to the company where accounts or information was misused and only reported elsewhere if the incident went unresolved or if they were advised to do so. This reporting trend could thus function to support fraudsters whose strategies often involve stealing small amounts from many victims rather than large amounts from a single victim (see Button and Cross 2017).

7.3.4 Qualitative Findings

The qualitative interviews revealed nuances that could not be captured in variable analyses. I found that victims’ reporting decisions often related to the ways that they understood incidents. For example, participants framing incidents as minor inconveniences were unlikely to escalate them to police or credit bureaus. In contrast, those framing incidents as relational issues opted not to report and instead dealt directly with the perpetrator, while those who saw incidents as institutional failures or breaches often closed accounts or stopped using institutions in lieu of formally reporting.

Interviews also revealed that emotional consequences were common in the aftermath of identity theft, including panic and embarrassment. When participants panicked, they often reported to the institution where accounts or information were misused, but they normally did so
quickly. In contrast, several participants expressed forms of embarrassment and self-blame and were less likely to disclose incidents to family based on anticipated reactions. Some, like Nolan, even delayed reporting to institutions due to embarrassment. This is in line with past interactionist contributions to the study of emotion, which have argued that role-taking emotions like embarrassment can inform choices of actions and disclosure (Goffman 1963; Schott 1979). This also ties to past research finding that victim-blaming discourses surround fraud victims (Cross 2015), a consequence of which can be decreased help-seeking (Cross 2018b). As such, this finding merits attention since victims may be less likely to seek advice from others or assistance from institutions due to the perception that they would be judged. In the present study, the victims who reported embarrassment eventually sought help; nonetheless, these emotions can function as a barrier to recuperating losses.

Participants provided many reasons for not reporting to police, including that it would create more work. Whitson and Haggerty (2008) argued that individuals are made responsible for both protection against identity theft and, when victimized, its resolution. Victims’ reporting options regularly involve automated systems and under-staffed helplines (see Whitson and Haggerty 2008), and participants in this study often described long wait times. Although all of the participants who cited the additional work as reasons for not reporting were eventually reimbursed through companies, this involved significant time commitments. For example, Courtney began by calling credit issuers one-by-one before contacting a credit bureau and completing additional paperwork for the many credit products opened in her name. Similarly, Edward described calling Amazon about 20 times. When victims are forced to spend countless hours contacting companies and credit bureaus, the time commitment of identity theft
victimization appears to function as a deterrent to police reporting. Nonetheless, identity theft victims continue to depend on private companies for reimbursement, and it appears that victims’ additional work is often a direct by-product of institutions’ fraud and assistance policies.

Finally, an interesting qualitative finding from the interviews was that participants often followed the advice of institutional actors, yet the advice they received varied substantially. For example, Courtney had several credit products opened in her name and began calling them one-by-one. After speaking to multiple companies’ agents, one eventually recommended that she contact a credit bureau to better understand the scope of the issue. To Courtney, this advice seemed like the correct course of action, yet other company agents had not recommended contacting a credit bureau. This suggests that victims of identity theft are likely to receive different advice depending on the company that they call or the agent to whom they speak. Another example is Hunter, who experienced two incidents, one of which was the result of a phishing scam. After the phishing scam, she only reported to her financial institution and took no further action, recalling that the bank did not recommend contacting a credit bureau. The only other victim of a phishing scam that I spoke to, Dalton, had his financial institution contact a credit bureau and go through his report with him. Moreover, because the nature of phishing scams involves giving up personal information, checking one’s credit report can be worthwhile. In sum, the advice received from institutional actors varied, yet it was often followed and cited as a reason that participants seldom escalated cases to credit bureaus or law enforcement.

7.4 The Resolution of Identity Theft

In answering this study’s final research question about victims’ satisfactions with the institutions contacted, I found that victims’ experiences varied substantially even when the
characteristics of the incidents were somewhat similar. Although this is a relatively straightforward argument on the surface, it merits further discussion in the context of this study’s finding that victims’ understandings of incidents can be processes and past findings about the differential effect of victimizations.

First, I found that participants who were made aware of incidents by their financial institutions typically had more positive experiences with reporting. Being notified about incidents in this way often meant that investigations would be more expedient, and it is expected that since the institution had already flagged the transaction as suspicious, victims would be more satisfied with its resolution. Moreover, where participants were made aware by other means, they were often satisfied if companies resolved the incident quickly. The most common complaints about institutions were that participants were referred elsewhere or that institutional actors seemingly did not care. These reasons for satisfaction and dissatisfaction are similar to those cited by fraud victims in the UK and Australia (see Button et al. 2009; Cross, Richards, and Smith 2016).

The results suggest that participants’ experiences with institutions varied widely even when accounting for differences in the characteristics of incidents. Based on the information that victims had about their incidents and their resolutions, the reasoning behind these differences can only be speculated. For example, Edward and Peter both had their Amazon accounts misused. Edward’s account was misused to purchase expensive electronics, he contacted Amazon immediately while the charge was pending, and the order was to be shipped to a newly added name and address. In contrast, Peter’s charges were for an Amazon gift card and he contacted the company as soon as he noticed, but not as soon as the charges were placed. While Peter’s order
was reimbursed within a ten-minute phone call, Edward’s took over a month to resolve. A better understanding of Amazon’s rules and procedures would be required to know why these experiences were so different. For example, it could be that Edward’s account misuse was less believable to employees because his entire computer was taken over, or it could be that employees have the power to reimburse gift card orders immediately.

Moreover, there was no clear connection between the complexity of cases and how satisfied victims were with their resolution. While Edward’s case may be viewed as complex since his computer was hacked and Marshall’s phone port represents an emerging form of identity theft that may require complex resolutions, victims with more straightforward incidents expressed similar dissatisfaction with institutions. Grant’s case seemed simple: he had used the food delivery company once, years prior, then he received an e-mail stating that his password had been changed. The next day, he noticed almost a thousand dollars in two charges from restaurants in the United States. After reporting to the delivery company and his credit card company, both institutions failed to reimburse him immediately and the incident took several weeks to be resolved. His experience appears unlucky compared to others, such as Regan, who had four thousand dollars taken and her phone ported out yet was reimbursed quicker and expressed satisfaction.

Finally, on its surface, Winston’s case of tax fraud appears to suggest that the complexity of a case contributes to dissatisfaction. It would be logical that because his case was complex, institutions struggled to resolve it and he was less satisfied with the resolution. However, the causal ordering is unclear, and it may instead imply that institutions play a role in informing the perception of a case’s complexity. Winston’s experience with the misuse of his tax account
appears complex because of the many institutional actors that he contacted to solve the issue: several tax centers, law enforcement, credit bureaus, a lawyer, and financial institutions. Eventually, he found one individual at a tax center who was able to resolve his ongoing issues, even though CRA agents had routinely referred him to other divisions, seemingly not knowing either how to or who could resolve the issue. Accordingly, had the first agent referred Winston to the appropriate individual, perhaps we would understand this incident as less complex. Thus, the causal ordering between perceived complexity and satisfaction with institutions could be bidirectional: the fact that so many institutional actors were unaware of what to do or how the incident occurred may have led him to see this case as more complex.

Similarly, the variation in participants’ experiences with institutions may be unexplainable based on the limited knowledge victims have about their incidents. Past research has indicated that few victims know about the origin of their incidents or their perpetrators (Harrell 2019; Turville et al. 2010). Nonetheless, several victims, like Grant and Logan, were dissatisfied with the lack of information they received from institutions. From the conversations I had, few victims were told new information about the origin of charges, such as the method of payment or the reason investigations confirmed that it was fraudulent. Although some victims were not concerned with receiving this information, others were. Where victims received little information about the origin of their incidents, a better understanding of the institution’s procedures may be required to explain the variations that victims experienced in terms of how quickly incidents were resolved.

Additionally, it is significant for identity theft prevention that victims reported a lack of closure about incidents following resolution. Although individuals are constructed by North
American institutions as responsible for their own protection against identity theft (Cole and Pontell 2006; Whitson and Haggerty 2008), they often receive little information from institutions about how incidents occurred. In turn, victims may be at ongoing risk for the same type of identity theft if institutions offer them no advice.\footnote{Like other crimes, some evidence exists that identity theft victims are at increased risk of repeat victimization (see Newman and McNally 2005), however defining and measuring repeat victims is complex for identity theft. One’s information can be taken once and misused in multiple ways or taken then reproduced and misused repeatedly over time.}

Finally, victims’ varied experiences with institutions may relate to past research on the differential effects of identity theft. Research has found that both financial (Copes et al. 2010; Reynolds 2021; van Wilsem et al. 2021) and emotional (Deem 2000) consequences vary based on factors unrelated to the incident itself, including demographics and social support. For example, Reynolds (2021) found that even when controlling for whether victims contacted financial institutions, those with lower incomes, lower educational attainments, and those who were unmarried were more likely to suffer out-of-pocket losses because of identity theft victimization. Reynolds (2021) speculated that one possible explanation for this finding was that those sociodemographic groups may have more difficulty receiving support from institutions. In line with this research, the diverse experiences with institutions could result from variations in how individuals are perceived by company actors. Some victims may receive improved responses from institutions if they have longer histories or more business with companies, and some institutions may benefit more from meeting the needs of customers with higher incomes. Further research is needed to better understand the reasons for the variation in victims’ reporting experiences.
7.5 Policy Implications

This study’s findings have many implications for policy, primarily related to victim assistance in the aftermath of identity theft. With some victims paying out-of-pocket for identity theft losses, others having to repeatedly call institutions for responses, and few incidents being recorded in police-reported crime statistics,\(^{50}\) the Canadian Government could better clarify the roles of responding institutions, including law enforcement. Although the Canadian Anti-Fraud Center (CAFC; 2021) recommends that victims report to local police, participants described past experiences of police being disinterested in responding to identity theft, fraud, and scams. If police only respond to specific types of identity theft and fraud, messaging should make that clear. At present, many institutions take responsibility for certain cases but not others, which enables the conditions for victims to be passed from one institution to another and to go unassisted.

Many improvements could still be made within current institutional arrangements. For example, law enforcement could respond to victims and, even if they do not investigate the case, they could ensure victims are put in touch with an organization that can assist. Moreover, as described in Chapter 6, many victims reported first to the institutions or companies where their accounts or information were misused, then only reported further if they were not reimbursed or if those companies recommended that they do so. Participants often described trusting the advice from institutional actors, which is concerning given that participants received inconsistent advice.

---

\(^{50}\) For example, fewer than 30,000 cases were recorded in police statistics in 2020 (Moreau 2021), despite 1.7 million Canadians estimated to be victimized in the last Canadian victimization survey (Sproule and Archer 2008), which occurred prior to identity theft’s criminalization and regular increases in police reported rates (Allen 2018; Moreau 2019; Moreau 2019).
on subsequent actions to take. Based on these experiences, it appears that institutions either do not have set advice to provide victims based on the circumstances of the incident, or that institutional actors are not offering that advice consistently. As such, institutions should have consistent and clear policies regarding the advice given to victims about their subsequent actions. These recommendations could be created based on advice from security experts but may include conditions under which victims should report elsewhere (e.g., checking their credit report in cases where victims provide information through a phishing scam). Based on the experiences of participants who were victimized by parents, institutions could also provide better proactive advice on how children’s accounts should be managed as they become adults.

Based on the varied responses victims received from supporting institutions, policy could better ensure that consumers are protected from institutions’ non-responses when retail and payment accounts are misused. Institutions apparently have very different procedures for handling incidents; thus, if victims are referred from institution to institution, they may fall through the cracks of victim support. Accordingly, responsibility cannot only fall on individual consumers or companies, who may be motivated to provide inadequate customer support (see Whitson and Haggerty 2008). Instead, the CAFC or another government body could serve as a unit that advocates for victims who fail to be supported by companies and institutions. Depending on the characteristics of the complaint, this entity could provide tailored advice to victims, contact institutions on behalf of victims who receive no responses, or provide other victim support or compensation.

This study also found that some victims felt that the reporting processes could be more straightforward. In Canada, the reporting recommendations are contained on the CAFC webpage,
which may be helpful for the victims who find it. However, because different forms of fraud may require vastly different actions, it may be beneficial to implement a tool similar to that on the American Federal Trade Commission (FTC) webpage, where victims can enter details of their incident and receive personalized recommendations. In the United States, reporting recommendations could be more consistent among the resources available, since the FTC, Homeland Security, and Internet Crime Complaint Center (IC3) provide different reporting options and unspecified recommendations for incidents fitting multiple categories.

Policy could also be implemented to support the victims who were hesitant to seek help due to embarrassment or anticipated reactions, as well as those victims who blamed themselves. These findings are concerning in the context of past research, which indicates that responsibility for identity theft protection is placed on individual consumers (Whitson and Haggerty 2008) despite the frequency of widespread breaches and hacks of unsecure company and government databases (Monahan 2009). Where institutional messaging depicts victims as those who are unable to protect themselves, it follows that they may self-blame (Cole and Pontell 2006) and thus be less likely to report to institutions. A complete reversal of messaging from government and law enforcement would be ideal, but at the very least, they could provide messaging that aims to reduce embarrassment and fear of anticipated reactions when victimized.

7.6 Directions for Future Research

Moving forward, research on identity theft experiences should increase in several manners. In Canada, representative victimization surveys are desperately needed to understand the scope of the issue. While the 2009 General Social Survey on victimization included questions about whether respondents had personal information leaked or experienced phishing attacks
(Statistics Canada 2009), these questions were removed for the 2014 cycle\textsuperscript{51} (Statistics Canada 2021). Moreover, the most recent representative Canadian identity theft victimization survey (Sproule and Archer 2008) predates the assent of Bill S-4, which criminalized identity theft in Canada. With few incidents reported to law enforcement, little is publicly known about the scope of identity theft in Canada.

Simultaneously, research on identity theft should focus on individuals’ experiences and perceptions of the incidents. Outside of this project, little research has examined what fraud or identity theft mean to those experiencing it. This study suggests that misused accounts and identity information, which are events that could legally be defined as identity theft, can be understood within several social frameworks. Our knowledge of identity theft would benefit from further researching victimized and non-victimized citizens’ perceptions of identity theft, fraud, and misused accounts and identity information. Only then can researchers determine whether the definitions used by scholars and in law reflect those of everyday social dialogue.

Moreover, victims’ reporting experiences and decisions should be further investigated. In the United States, qualitative research would be beneficial to better understand whether and why participants reported to the FTC, local police, or other institutions. Identity theft victims who suffer out-of-pocket losses are currently not well understood. Although this study found that their reporting was impacted differently by measures of seriousness than those recuperating losses, future research could examine their experiences with reporting and the reasons they cannot

\textsuperscript{51} Other representative Canadian surveys, including Statistics Canada’s 2018 Canadian Internet Use Survey and private consumer fraud surveys (see Chartered Professional Accountants Canada 2020; Leger 2016), assess fraud incidents but fail to inform knowledge about the scope and nature of identity theft in Canada.
recuperate losses. Moreover, it would be helpful to further research whether victims of identity theft see the resources on the CAFC and FTC websites before reporting. Finally, based on the finding that some victims follow the advice of institutional actors, it would be beneficial to examine the identity theft and fraud policies, procedures, and recommendations of financial institutions, companies, credit bureaus, and law enforcement. This could include institutional ethnographies or interviews with institutional actors at various levels within responding organizations.

While I would like to eventually see the NCVS – ITS grow and, like the broader NCVS, include waves of surveys to better understand causality, I cannot recommend that before prioritizing the aforementioned research. Based on the present study, it remains unclear whether those reflected in the survey view their incidents as identity theft or themselves as victims. Instead of additions to the NCVS – ITS, qualitative research is needed to continue engaging with the public’s perceptions of identity theft and related phenomena. Qualitative insights can also enable an assessment of the validity of existing survey questions, thereby ensuring that survey items have the same meaning for researchers as they do for respondents. The ITS is a primary source of knowledge on identity theft victims and the scope of identity theft in North America, and it is important to ensure that it captures its intended responses.

### 7.7 Summary

In summary, victims’ conceptualizations of incidents are important because they do not always think of identity theft incidents as criminal, but sometimes as inevitable, as relational issues, as company failures, and more. This leads to further questions about why identity theft was criminalized if it is routinely treated as non-criminal. Participants often reported to
institutions based on how they understood the incident, but many saw their case as insufficiently serious for police, suggesting that the criminalization of identity theft has not reflected public perceptions of the crime. This may be due to the messaging from governments and institutions that place responsibility on individuals or due to informal experiences that individuals have with others, police, and company actors. Accordingly, it is concerning that many victims see these issues as appropriate for companies and financial institutions to resolve, yet these institutions provide varied support, with some victims describing negative experiences and having to repeatedly contact companies to be reimbursed.

The policy implications of these findings are that victims need better support. The process can be unclear, and companies seemingly have full autonomy over resolving incidents despite these individuals being victims of a crime. If companies and financial institutions are the security actors that the government wants to task with resolving the incidents they codified as criminal, then it follows that they should ensure that victims are not slipping through the cracks. Victim education and resources should also emphasize that feelings of self-blame and embarrassment are common among fraud victims (see also Cross 2005) and that victims should seek support from institutional actors regardless.

Future research is needed to examine the experiences of victims and the perceptions of non-victims in Canada and the United States. Moreover, research should focus on assessing the scope and nature of identity theft in Canada, given the relative lack of studies of Canadian victims since its criminalization.
8 Conclusion

8.1 Summary: Reflecting on the Research Questions

I started this project with the goal of better understanding why so few identity theft incidents come to the attention of law enforcement. With an absence of representative identity theft victimization surveys in Canada since its codification into the Canadian Criminal Code, I was struck by how little we know about the scope of the problem, and I looked at police reporting for answers. Something did not add up: prior to its criminalization, Sproule and Archer (2008) estimated that 1.7 million Canadians were victim to identity theft in a year, yet a decade later, official statistics were reporting fewer than 20,000 cases annually (Allen 2018; Moreau 2019).

The background literature on identity theft victim reporting is primarily quantitative, with most qualitative contributions coming from international studies of fraud victims. It is clear from past research that so-called cybercrimes are policed differently: private companies, security firms, and police all have some role in the security landscape (Nhan 2010). However, it was not clear whether citizens and potential victims saw these events in the same way as researchers: do people think of identity theft as a cybercrime and do they think of cybercrime as something that is policed differently? I wanted to start at the start. I developed the following research questions:

1. a) How do those who have experienced identity theft understand the events – be it as crimes, inconvenient events, or otherwise?
   b) Do those who experience identity theft victimization identify themselves as victims of crime?
2. a) Do those who have experienced identity theft formally report it? If so, to whom?
   b) Why do those who have experienced identity theft choose to report or not report to specific institutions (e.g. police, credit card company, etc.)?
3. How satisfied are victims with the resolution facilitated by the institutions they approach?
I set out to talk to victims of identity theft to answer my research questions. Simultaneously, I was entranced by the discussion about whether victims of identity theft were actually victims if they recuperated losses (see Koops and Leenes 2006). I decided to perform a mixed methods study where I could analyze out-of-pocket loss as a potential moderating variable in reporting and then build on this research through qualitative insight. I was inspired by the recruiting methods of Emerson, Ferris, and Gardner’s (1998) study of stalking victims to recruit participants that could be defined as identity theft victims but who may not see themselves and the incidents as such.

As with any project of this length, more contributions arose as I progressed through the interviews, data analysis, and writing. Some recent studies were particularly informative and inspiring: Button et al. (2021) examining cybercrime victims’ perceptions of seriousness; Cross and Layt (2021) studying romance fraud, including the importance of internet searches to fraud awareness; and Green et al. (2020a; 2020b) and Geis et al.’s (2021) projects interviewing victims who contacted the Identity Theft Resource Center. In many ways, the research described in the literature review may have logically led to slightly different research questions, or sub-research questions, had I begun today.

Through the interviews, I found that victims of identity theft generally understand, at least when probed, that the misuse of their accounts or identity information is a crime. They generally admit, at least when probed, that they are victims, but they often rationalize that they did not face much harm or were somehow partially to blame. But when they talk freely about what happened to them, about when their identity information or accounts were misused, they talk about much more than just crimes. Some victims see these events as inevitable
inconveniences of life today, others see these as relational issues, and still others see these incidents as company failures, breaches, or even mistakes. Moreover, their perceptions of the events change, sometimes completely reversing from crime to non-crime, as they learn new information: by talking to institutional actors; by searching the web; by checking their credit; or by simply waiting to discover if subsequent misuses occur.

As for reporting, the quantitative results show that out-of-pocket loss has a moderating effect on other measures of seriousness as they relate to police and credit bureau reporting. Those who pay out of pocket are more likely to report to police, and those who recuperate losses are more likely to report if they experience severe distress or spend longer dealing with the issue.

With respect to the interview results, only two participants reported to police, and in very different contexts. Instead, participants often only took the steps that were practical based on the way they understood the events that happened. Those who saw the incident as an inconvenience or only technically a crime reported it to the relevant institution and only reported further if it was recommended or went unresolved. Those who saw it as a relational issue did not report it: they dealt with it as a relational issue. Those who understood the event as a breach or a security failure often closed accounts or avoided institutions where the incident occurred rather than reporting.

Finally, while some victims were satisfied with their reporting experiences, others had as much or more frustration dealing with banks, credit card companies, or other institutions than they did with the incident itself. Some had to call institutions for weeks or months, some placed calls that were never returned, and others had difficulty finding anyone who was willing to help. Finally, some participants felt that the banks and other institutions provided no closure about the
incidents, leaving them confused as to how incidents occurred or how they could be prevented in the future.

8.2 Contributions

Although trends in identity theft reporting have been examined quantitatively, this study expands on these findings while contributing qualitative insight into the processes of reporting decisions and how people understand these incidents. The qualitative findings offer several important contributions to research on identity theft victims. Our understanding of identity theft victimization is enhanced by the knowledge that victims conceptualize the misuse of their accounts or identity information in several ways, not only as crimes and inevitable inconveniences, but also as relational issues, mistakes, and institutional security failures. In this sense, the symbolic interactionist approach to victimization revealed that the meanings victims derive from criminal events vary and that these meanings can inform whether and from whom individuals seek help. The symbol ‘identity theft’ has been popularized in North America following the codification of identity theft laws\textsuperscript{52} that banned the misuse of accounts and identity information, yet when faced with these events, victims may understand incidents and themselves in vastly different ways. Moreover, victims only sometimes see these incidents as identity theft or as crimes at all. Given that close to ten percent of North Americans are victimized annually, it is important that victims may not see these incidents as crimes, particularly when cases are reported to police at lower rates than victims are paying out-of-pocket for identity theft losses (see Harrell 2019).

\textsuperscript{52} Along with its increasing prominence in news, political discourse, and popular media.
Relatedly, victims often report to the institutions that they see as practical for resolving the type of incident they understand their fraud to be. Many victims opted not to report to police when they viewed incidents as only minor inconveniences: they saw a disconnect between the incident they experienced and the type of incident to which police are suitable to respond. The finding that victims’ understandings of events can impede their reporting contributes to the literature since reporting is often examined quantitatively and explained as a rational choice decision based on incident seriousness (see Xie and Baumer 2019). Due to the underreporting of identity theft and the lack of representative victim surveys, we do not know the scope of identity theft in Canada. In fact, it is likely that financial institutions have better awareness of the total number of Canadians victimized annually than do law enforcement. Moreover, many victims followed the reporting advice of institutional actors, yet the advice afforded to victims varied based on the company or individual that they reached.

This study also contributes to the existing body of literature by finding that many identity theft victims resist full identification with the victim label by downplaying the harm they experienced or by identifying themselves as somewhat responsible for their victimization. Knowing that some victims deny that they faced harm because they recuperated losses enhances our understanding of identity theft in society, as it suggests that many individuals normalize or rationalize the distress experienced and the time spent resolving incidents. That victims themselves downplay emotional costs and lost time simply because they do not have financial costs represents a normalization of the often-strenuous process of recuperating losses. As Whitson and Haggerty (2008) aptly observed, “lost in this catalogue of bureaucratic ineptitude…
is recognition that there is nothing natural and inevitable about bureaucratic inefficiencies” (p. 591).

Moreover, some participants who were victimized by their parents resisted the victim label due to their perception that they had some role in the incident. During his interview, Ian and I discussed how it is common for parents to have access to their children’s account information when they are young: children often need their parents to open accounts, and parents usually teach their children how to use bank accounts and credit cards. Thus, parents are typically trusted figures in the process of individuals’ becoming embedded in modern payment systems. It is therefore troubling when those who are victimized by parents blame themselves for identity theft incidents because they trusted their parents with account information. Moreover, these victims are less likely to seek formal support, and thus they could be more likely to face out-of-pocket costs since their only chance at reimbursement is recuperating money from their parents. While this sample had a disproportionate number of participants victimized by parents, these findings are significant for understanding a subset of victims who may need additional support. They also suggest that financial institutions could better educate parents and families on how to transition from holding joint accounts to individual ones.

Tied to interactionist literature on role-taking emotions (Shott 1979), this research also found that embarrassment may function as a barrier to help-seeking for victims of identity theft. Cross (2015) identified that victim-blaming discourses surround victims of romance, advance-fee, and phishing fraud, all of which require a victim to respond to the perpetrator and thus depict victims as having an active role in the events. This study advances the literature by finding that several participants with misused accounts expressed embarrassment when disclosing to family
or institutional actors, even when the fraud did not result from phishing. This may relate to the discourses surrounding identity theft, which past research has found places responsibility on individuals for their own protection (Cole and Pontell 2006; Whitson and Haggerty 2008).

By examining how measures of seriousness and situational variables impact reporting to law enforcement, financial institutions, and credit bureaus, this study builds on quantitative findings that some measures of seriousness increase the likelihood that incidents are reported to law enforcement (Reyns and Randa 2017). This study also contributes by identifying the time spent resolving issues as a significant consequence impacting reporting decisions. Moreover, while out-of-pocket loss has been identified as a strong predictor of reporting to law enforcement (Reyns and Randa 2017), the interaction effects in this study suggest that victims who suffer out-of-pocket losses may have different predictors for reporting to institutions. For example, while victims who recover losses are more likely to report to police when they experience severe distress or greater losses of time, victims who pay out of pocket are more likely to report regardless of other measures of seriousness. This is supported by interview findings, where victims frequently rationalized non-financial costs as miniscule when they recovered losses. These findings contribute to past research and suggest that victims are first concerned with recuperating losses, then with dealing with the incidents promptly and without distress. Finally, these findings offer support for examining those who suffer out-of-pocket losses as a distinct group of identity theft victims with different motivations for reporting to law enforcement and credit bureaus than those who recover losses.

Finally, this study found that victims’ satisfaction and experiences with the institutions they contact for assistance vary widely. Although negative experiences of fraud victims have
been noted internationally (Button et al. 2009; Cross, Richards, and Smith 2016), this research is the first in Canada to examine victims’ satisfaction with the fraud justice network. Like their international counterparts, Canadian victims sometimes receive empty promises about further contact from institutions, must repeatedly call institutions, or are redirected elsewhere. In some cases, victims’ experiences suggest that some institutional actors may not know the proper ways to resolve identity theft, since some redirect victims to departments that do not resolve the incident, while others provide conflicting advice. Finally, institutional responses are found to often leave victims desiring more information, which is significant given the importance that is placed on individuals to protect themselves.

8.3 Limitations

A main limitation of this study’s design was using survey responses from a representative American sample and qualitative interviews with participants from Southern Ontario. As discussed in the literature review, although the laws in both countries are similar, online advice to victims of identity theft varies considerably. The goal of using multiple methods was to produce complementary insights about identity theft reporting in North America. Accordingly, the qualitative findings do not explain the quantitative results or vice versa; rather, both contributions are exploratory in nature given the limited research on identity theft victims’ reporting upon which this study builds. Although each method produced contributions to knowledge about identity theft victims’ reporting decisions, the strengths of each method do not
necessarily lead to a stronger study. Along with more contributions to knowledge enabled by mixing methods came a greater set of limitations to address.

A primary concern of interactionist research is ensuring that concepts and interpretations reflect the social world being studied, which quantitative approaches may neglect (Blumer 1969). While the tenets of interactionism are compatible with quantitative analyses (see Couch 1958; Fine 1993; Heise 1977; Kuhn and McPartland 1954; Maines 2003; Ulmer and Wilson 2003), interpretations of variable analysis using the NCVS – ITS data are only important insofar as they reflect the same meaning held by survey respondents. I have tried my best to keep variable names and discussions of variables as close as possible to the way the questions were asked to respondents, but some variables merit further attention.

For example, there remains some ambiguity regarding what actions would constitute reporting in respondents’ perspectives. For example, some respondents may call police to ask for advice, while others may complete police reports. With respect to financial institutions, an independent variable included in the analysis was whether participants found out about incidents by being notified by their financial institutions. Whether or not one reported to their credit card company or bank may not be clear when the victim received a call from that institution notifying them of potential fraud. While it is suspected that respondents would only answer positively to reporting when they contacted the institution, rather than vice versa, this cannot be known with certainty. Moreover, this may be a unique issue for identity theft victim surveys considering the many ways that individuals may discover that an incident has occurred.

53 See Hesse-Biber (2015) for a discussion of the common misconception that mixed methods research naturally produces findings greater than the sum of each component.
Additionally, some variables produced limited knowledge about the characteristics of identity theft incidents. For example, the variable capturing whether the victim knew their offender is based on a question that asks if they knew anything about the person who misused their information. Not only does this provide little information about the nature of the relationship, but it remains unclear at what point a respondent would answer affirmatively.

Finally, given the little existing data on identity theft victims, the quantitative data used were cross-sectional, and thus the direction of some relationships remains unclear. For instance, out-of-pocket loss may be associated with a decreased likelihood of having contacted financial institutions either because of the increased complexity of these incidents or because victims who contacted financial institutions were assisted in recuperating their losses. Similarly, distress may have resulted from both the incident itself and the interactions with institutional actors when attempting to resolve incidents. Nonetheless, these associations are useful to understand as a starting point for causal research.

Of course, the qualitative interviews were not free from limitations either. One limitation is the use of both in-person and telephone interviews, as it is possible that participants respond differently face-to-face and on the phone. The option for phone interviews was initially provided to accommodate participants who were too busy to meet in person, but following the onset of the COVID-19 pandemic, all interviews were conducted over the telephone. Non-verbal communication can be key during participants’ narratives, and despite verbal prompts, it is possible that some participants would have provided more detail in person. Additionally, during telephone interviews, it was sometimes difficult to gauge whether it was appropriate to play devil’s advocate or challenge the participant’s responses.
The onset of the pandemic may have also dictated the type of person who had time to participate. While those temporarily out of work may have had more time to participate, others may have been working longer hours in essential jobs, thus being unable to participate. Moreover, in line with other North American studies of identity theft victims, exhaustive demographic information was not collected from participants due to concerns over having them share identity information (see Green et al. 2020b). In turn, while the interviews offer insight into the experiences of victims in Ontario, certain sociodemographic groups or forms of fraud may be overrepresented.

In summary, both the quantitative and qualitative findings have limitations, and the inferences drawn from the results should be contextualized. Nonetheless, the contributions described previously are significant in the context of the limited existing research on identity theft, and future research can strive to further expand on this knowledge.

### 8.4 Final Thoughts

Identity theft impacts millions of North Americans annually in countless ways. In Canada, we have not had estimates of the total number impacted by identity theft in over a decade, nor do we know its consequences. Our last representative victimization survey estimated that 1.7 million Canadians were impacted (Sproule and Archer 2008). Borrowing from our neighbours to the south, we can assume that identity theft has similarly increased since then. In the United States, 12 percent of victims paid out-of-pocket for losses in 2016, yet only 7 percent reported to police (Harrell 2019). Compound this with the fact that identity theft disproportionately impacts those with fewer resources to overcome it (Reynolds 2021; van Wilsem et al. 2021), and it seems like a problem worthy of attention. Yet this research found that
some Canadian victims do not see identity theft as a crime, and even more do not see it as a matter for police. In fact, less than 30,000 identity theft and fraud cases were reflected in police statistics in 2020 (Moreau 2021), fewer than two percent of a conservative estimate of total cases. The government, scholars, and the public know very little about the scope and nature of identity theft in Canada.

Of course, some victims recover losses quickly and painlessly because companies or their financial institutions help. Other victims, like Dalton and Benjamin, have paid thousands of dollars out of pocket. Still others, like Winston, have been dealing with their misused accounts for over a decade, including sometimes spending hours seeking help every night after work. Out of the twenty participants I spoke to, two paid out-of-pocket for their losses, most reported considerable distress, some had relational rifts, one lost their dream job opportunity, one lost trust in all healthcare institutions, one had their post-secondary education severely impacted, and many felt, at least at times, that there was no institution that would help. With the limited existing scholarship and data on identity theft in Canada, we do not even know the relative prevalence of these cases and consequences. Ultimately, while victims understand these events in various ways and report accordingly, the toll and scope of identity theft must be better understood so that victims can be better assisted.
REFERENCES


222


223


Canadian Victims Bill of Rights. Statutes of Canada 2015, Chapter 13, Section 2.


## APPENDICES

### Appendix A: Coding for the Quantitative Variables in this Study

<table>
<thead>
<tr>
<th>Variable</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dependent Variables</strong></td>
<td></td>
</tr>
<tr>
<td>Report to Law Enforcement</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td>Report to Financial Institution</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td>Report to Credit Bureau</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td><strong>Measures of Seriousness</strong></td>
<td></td>
</tr>
<tr>
<td>Amount Taken</td>
<td>Logarithmic Dollar Value</td>
</tr>
<tr>
<td>Out-of-Pocket Loss</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td>Distress</td>
<td>1 = Not at All Distressing</td>
</tr>
<tr>
<td></td>
<td>2 = Mildly Distressing</td>
</tr>
<tr>
<td></td>
<td>3 = Moderately Distressing</td>
</tr>
<tr>
<td></td>
<td>4 = Severely Distressing</td>
</tr>
<tr>
<td>Time Spent Resolving Incident</td>
<td>1 = One Day or Less</td>
</tr>
<tr>
<td></td>
<td>2 = &gt; One Day, but &lt; One Week</td>
</tr>
<tr>
<td></td>
<td>3 = ≥ One Week, but &lt; One Month</td>
</tr>
<tr>
<td></td>
<td>4 = ≥ One Month, but &lt; Three Months</td>
</tr>
<tr>
<td></td>
<td>5 = ≥ Three Months, but &lt; Six Months</td>
</tr>
<tr>
<td></td>
<td>6 = ≥ Six Months, but &lt; One Year</td>
</tr>
<tr>
<td></td>
<td>7 = One Year or More</td>
</tr>
<tr>
<td><strong>Situational Variables</strong></td>
<td></td>
</tr>
<tr>
<td>Previous Identity Theft Victimization</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td>Knowledge about the Offender</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td>Knowledge of How Personal Information was Obtained</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td>Length of Time Personal Information Misused</td>
<td>1 = One Day or Less</td>
</tr>
<tr>
<td></td>
<td>2 = &gt; One Day, but &lt; One Week</td>
</tr>
<tr>
<td></td>
<td>3 = ≥ One Week, but &lt; One Month</td>
</tr>
<tr>
<td></td>
<td>4 = ≥ One Month, but &lt; Three Months</td>
</tr>
<tr>
<td></td>
<td>5 = ≥ Three Months, but &lt; Six Months</td>
</tr>
<tr>
<td></td>
<td>6 = ≥ Six Months, but &lt; One Year</td>
</tr>
<tr>
<td></td>
<td>7 = One Year or More</td>
</tr>
<tr>
<td>Victim Made Aware by Financial Institution</td>
<td>0 = No</td>
</tr>
<tr>
<td></td>
<td>1 = Yes</td>
</tr>
<tr>
<td><strong>Demographic Variables</strong></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>Years</td>
</tr>
<tr>
<td>Household Income</td>
<td>1 = &lt;$5,000</td>
</tr>
<tr>
<td></td>
<td>2 = $5,000–$7,499</td>
</tr>
<tr>
<td></td>
<td>3 = $7,500–$9,999</td>
</tr>
<tr>
<td></td>
<td>4 = $10,000–$12,499</td>
</tr>
<tr>
<td></td>
<td>5 = $12,500–$14,999</td>
</tr>
<tr>
<td></td>
<td>6 = $15,000–$17,499</td>
</tr>
<tr>
<td></td>
<td>7 = $17,500–$19,999</td>
</tr>
<tr>
<td></td>
<td>8 = $20,000–$24,999</td>
</tr>
<tr>
<td></td>
<td>9 = $25,000–$29,999</td>
</tr>
<tr>
<td></td>
<td>10 = $30,000–$34,999</td>
</tr>
<tr>
<td></td>
<td>11 = $35,000–$39,999</td>
</tr>
<tr>
<td></td>
<td>12 = $40,000–$49,999</td>
</tr>
<tr>
<td></td>
<td>13 = $50,000–$74,999</td>
</tr>
<tr>
<td></td>
<td>14 = $75,000 and Over</td>
</tr>
<tr>
<td>Education</td>
<td>1 = Less than High School</td>
</tr>
<tr>
<td></td>
<td>2 = High School Graduate</td>
</tr>
<tr>
<td></td>
<td>3 = Some College</td>
</tr>
<tr>
<td></td>
<td>4 = Associate or Bachelor’s Degree</td>
</tr>
<tr>
<td></td>
<td>5 = Advanced Degree</td>
</tr>
<tr>
<td>Gender</td>
<td>0 = Male</td>
</tr>
<tr>
<td></td>
<td>1 = Female</td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td>1 = White</td>
</tr>
<tr>
<td></td>
<td>3 = Hispanic/Latinx</td>
</tr>
<tr>
<td></td>
<td>2 = Black</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>Marital Status</strong></td>
<td>0 = Unmarried</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td>1 = Northeast</td>
</tr>
<tr>
<td></td>
<td>2 = Midwest</td>
</tr>
</tbody>
</table>
Appendix B: NCVS – ITS Questionnaire

The questionnaire below includes all the variables examined in the quantitative analyses. All questions herein are from the National Crime Victimization Survey: Identity Theft Supplement, 2016 Codebook (United States Department of Justice 2016). The first five questions about specific types of identity theft are the ITS inclusion criteria.

<table>
<thead>
<tr>
<th>Variable:</th>
<th>Question:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misuse of Bank Account</td>
<td>During the past 12 months, since (reference period start date; 12 month reference period), has someone, without your permission, used or attempted to use your existing checking or savings account, including any debit or ATM cards?</td>
</tr>
<tr>
<td>Misuse of Credit Card</td>
<td>Since (reference period start date; 12 month reference period) has someone used or attempted to use one or more of your existing credit cards without your permission? Please do not include debit cards.</td>
</tr>
<tr>
<td>Misuse of Other Account</td>
<td>Since (reference period start date; 12 month reference period) has someone misused or attempted to misuse another type of existing account such as your telephone, cable, gas or electric accounts, online payment account like Paypal, insurance policies, entertainment accounts like iTunes, or something else?</td>
</tr>
<tr>
<td>Opening of New Account</td>
<td>Since (reference period start date; 12 month reference period), has someone, without your permission, used or attempted to use your personal information to open any NEW accounts such as wireless telephone accounts, credit card accounts, loans, bank accounts, online payment accounts, or something else?</td>
</tr>
<tr>
<td>Other Fraudulent Misuse of Personal Information</td>
<td>Since (reference period start date; 12 month reference period), has someone used or attempted to use your personal information for some other fraudulent purpose such as getting medical care, a job, or government benefits; renting an apartment or house; giving your information to the police when they were charged with a crime or traffic violation, or something else?</td>
</tr>
<tr>
<td>Report Police</td>
<td>Did you contact any law enforcement agencies, such as the local police, a sheriff or a federal law enforcement agency, to report (the most recent/the) misuse or attempted misuse of your personal information?</td>
</tr>
<tr>
<td>Report Financial Institution</td>
<td>Were you in contact with anyone at a credit card company, bank, or other financial institution about (the most recent/the) misuse or attempted misuse of your personal information?</td>
</tr>
<tr>
<td>Report Credit Bureau</td>
<td>Did you contact a credit bureau about the misuse or attempted misuse of your personal information?</td>
</tr>
<tr>
<td>Amount Taken</td>
<td>What is the approximate total dollar value of what someone obtained during (the most recent/the) incident of the misuse or attempted misuse</td>
</tr>
<tr>
<td>Question</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Personal Financial Loss</td>
<td>Of this ($ Total Loss) that was obtained during (the most recent/the) misuse of your personal information, how much of that money did you personally lose? That is, how much did you lose that was not covered or reimbursed by insurance or a credit card company?</td>
</tr>
<tr>
<td>Distress</td>
<td>How distressing was the misuse or attempted misuse of your personal information to you? Was it not at all distressing, mildly distressing, moderately distressing, or severely distressing?</td>
</tr>
<tr>
<td>Time Spent Resolving</td>
<td>How long did it take you to clear up all of the financial and credit problems associated with the misuse after you discovered it?</td>
</tr>
<tr>
<td>Prior Identity Theft Victimization</td>
<td>Outside of the past year, has anyone ever, without your permission: misused one of your existing accounts, used your personal information to open a new account, or used your personal information for some other fraudulent purpose, such as getting medical care, a job, government benefits or something else?</td>
</tr>
<tr>
<td>Know About Offender</td>
<td>Do you know, or have you learned, anything at all about (the most recent/the) person or person(s) who misused or attempted to misuse your personal information?</td>
</tr>
<tr>
<td>Know How Information Obtained</td>
<td>Do you have any idea of HOW your personal information was obtained, even if you are not completely certain?</td>
</tr>
<tr>
<td>Length of Time Information Misused</td>
<td>How long had your personal information been misused before you discovered it?</td>
</tr>
<tr>
<td>Made Aware by Financial Institution</td>
<td>How did you FIRST find out someone had misused or attempted to misuse your personal information?</td>
</tr>
</tbody>
</table>
Appendix C: Image of Recruitment Poster

The Use of Accounts or Identity Information without Consent

PARTICIPANTS NEEDED

If someone has benefited by using your personal information or one of your accounts without your consent, researchers at the University of Guelph want to hear about your experiences.

This includes if someone, without your consent:

- used your name or personal information to apply for social services or another benefit.
- opened a credit card, bank, utilities, or other account in your name.
- used your credit card, bank, utilities, or other account.

Participants will be asked to take part in a confidential 1-on-1 interview that may last up to 1.5 hours.

You would be asked about your experience with the misuse, how it affected you, and how you dealt with these problems.

All participants will receive a 20$ gift card for gas or groceries.

For more information, please contact Dylan Reynolds at dreyno06@uoguelph.ca

This study has received clearance from the Research Ethics Board at the University of Guelph (REB # 19-04-019).
Appendix D: Interview Participant Survey

This survey was administered to the interview participants prior to the open-ended interview. The questions are derived from the National Crime Victimization Survey: Identity Theft Supplement, 2016 Codebook (United States Department of Justice 2016).

1) Were you in contact with anyone at a credit card company, bank, or other financial institution about (the most recent/the) misuse or attempted misuse of your personal information?
   □ Yes
   □ No

   If “Yes”:
   After you told a financial institution that your personal information had been misused, how satisfied were you with their response?
   □ Very Satisfied
   □ Somewhat Satisfied
   □ Somewhat Dissatisfied
   □ Very Dissatisfied
   □ Neither Satisfied nor Dissatisfied

2) Did you contact a credit bureau about the misuse or attempted misuse of your personal information?
   □ Yes
   □ No

   If “Yes”:
   After you told a credit bureau that your personal information had been misused, how satisfied were you with the credit bureau's response?
   □ Very Satisfied
   □ Somewhat Satisfied
   □ Somewhat Dissatisfied
   □ Very Dissatisfied
   □ Neither Satisfied nor Dissatisfied

3) Did you contact any law enforcement agencies, such as the local police or the RCMP to report (the most recent/the) misuse or attempted misuse of your personal information?
   □ Yes
   □ No

   If “Yes”:
   How satisfied were you with the law enforcement agency's response when you reported the misuse of your personal information?
   □ Very Satisfied
If you did not contact law enforcement:
We would like to learn more about why people who experience misuse of accounts or identity do not report it to law enforcement. Why did you decide not to contact a law enforcement agency? (MARK ALL THAT APPLY)
- Didn't know that I could report it
- Didn't think about reporting it
- Didn't know what agency was responsible for identity theft crimes
- I didn't lose any money/It was an attempt
- Not important enough to report/small loss
- Reported it to someone else such as a credit card company/bank/insurance company or other organization
- Took care of it myself
- Didn't think the police would do anything
- Didn't want to bother the police
- Didn't find out about the crime until long after it happened/too late for police to help
- Couldn't identify the offender or provide much information that would be helpful to the police
- I was afraid to report it
- The person responsible was a friend or family member and I didn't want to get them in trouble
- I was embarrassed
- Too inconvenient/didn't want to take the time
- Other (specify) __________________________

4) What is the approximate total dollar value of what someone obtained during (the most recent/the) incident of the misuse or attempted misuse of your personal information? Include the value of goods, services, credit, loans, cash, and anything else the person may have obtained.
______________________________

5) Of this ($ Total Loss) that was obtained during (the most recent/the) misuse of your personal information, how much of that money did you personally lose? That is, how much did you lose that was not covered or reimbursed by insurance, a credit card company, or another company?
______________________________

6) How long did it take you to clear up all of the financial and credit problems associated with the misuse after you discovered it?
□ One day or less (1-24 hours)
□ More than a day, but less than a week (25 hours-6 days)
□ At least a week, but less than one month (7-30 days)
□ One month to less than three months
□ Three months to less than six months
□ Six months to less than one year
□ One year or more

7) How distressing was the misuse or attempted misuse of your personal information to you? Was it not at all distressing, mildly distressing, moderately distressing, or severely distressing?
   □ Not at all distressing
   □ Mildly distressing
   □ Moderately distressing
   □ Severely distressing

8) Do you have any idea of HOW your personal information was obtained, even if you are not completely certain?
   □ Yes
   □ No
Appendix E: Interview Guide

1) Would you describe the ‘story’ of a time when you experienced an account or your identity being used by somebody without your consent?
   • Probe: What happened next?

2) Were there any other times that you experienced an account or your identity being used by somebody without your consent?

*Questions following the narrative phase will take into account the participant’s prior responses. Examples of potential probes and questions are presented.

3) When and how did you find out about the incident?
   • Do you remember how you felt when you learned about the incident?

4) Some of these were asked in the survey, but I’d like to get more detail:
   Do you have any idea of how your personal information was obtained, even if you are not completely sure?
   • Follow-up: If so, how was it obtained [or how do you believe it was obtained]?

5) Did you seek advice from anyone on what to do after the incident, including friends, family, or co-workers?
   • Follow-up: What was their advice?

6) People report these incidents to a variety of institutions, including: the local police, the RCMP, credit bureaus, a credit card company or bank, or another company. Did you report the incident to any of these groups?
   • Follow-up: Which? In-person, over the phone?
   • Follow-up: What was your experience with [institution contacted]?
   • How satisfied were you with how they helped resolve the incident?
   • Did you report to any other institutions?
   • Who was the most helpful during this time? Why?
   • What made you decide to report it to [this particular] institution?

7) The survey asked whether you reported to police or the RCMP and if no, why not. Did you want to add anything to the reasons why you did not report to RCMP?
   • Did you know about the Canadian anti-fraud centre? Did you know to report to them?

8) How did this experience impact you?
   • Financially? Time?
   • Emotionally / Relationally?
• Behaviorally, have you changed any purchasing or other behaviors since the incident?

9) What are your thoughts about the problem of the misuse of accounts or identity information in our society?
   • Is it something we just have to accept? OR
   • Should government agencies and police be taking it more serious to try to prevent it?
   • Whose responsibility is this issue?
   • Thinking back to before this incident, can you remember if it was something you gave much thought? Have your thoughts changed since before the incident?

10) Thinking about this past unauthorized use of [your account or your identity], do you consider yourself a victim of a crime?
    • Follow-up: Why or why not?
    • Follow-up (may include): In a legal context, you could be described as a victim of identity theft or identity fraud. What are your thoughts on these issues?
    • Do you have other thoughts on the word victim in this context?

11) Based on your experience with the unauthorized use of [your account or your identity], what would you recommend to someone who has just found out that their [account or identity] has been misused?
    • Probe: Who would you recommend they report it to?
Appendix F: Complete Logistic Regression Tables for Tests of Interaction Effects

Table 6-3: Logistic regression predicting identity theft victims reporting to law enforcement (n = 5,753)

<table>
<thead>
<tr>
<th></th>
<th>Model 6</th>
<th>Model 7</th>
<th>Model 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Pocket Loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>7.095 *</td>
<td>5.110 ***</td>
<td>7.610 **</td>
</tr>
<tr>
<td>Amount Taken (log)</td>
<td>1.527 ***</td>
<td>1.481 ***</td>
<td>1.476 ***</td>
</tr>
<tr>
<td>Time</td>
<td>1.251 ***</td>
<td>1.338 ***</td>
<td>1.240 ***</td>
</tr>
<tr>
<td>Distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not at All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mild</td>
<td>2.124 *</td>
<td>2.093 *</td>
<td>2.653 **</td>
</tr>
<tr>
<td>Moderate</td>
<td>2.581 **</td>
<td>2.517 **</td>
<td>3.380 **</td>
</tr>
<tr>
<td>Severe</td>
<td>3.022 **</td>
<td>2.928 **</td>
<td>4.767 ***</td>
</tr>
<tr>
<td>Out-of-Pocket Loss*Amount Taken (log)</td>
<td>0.818</td>
<td>0.734 **</td>
<td></td>
</tr>
<tr>
<td>Out-of-Pocket Loss*Time Spent</td>
<td></td>
<td>0.734 **</td>
<td></td>
</tr>
<tr>
<td>Out-of-Pocket Loss*Distress</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Not at All</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Mild</td>
<td></td>
<td></td>
<td>0.378</td>
</tr>
<tr>
<td>*Moderate</td>
<td></td>
<td></td>
<td>0.290</td>
</tr>
<tr>
<td>*Severe</td>
<td></td>
<td></td>
<td>0.148 *</td>
</tr>
<tr>
<td>Prior ID Theft</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>0.900</td>
<td>0.898</td>
<td>0.927</td>
</tr>
<tr>
<td>Know Anything About Offender</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>2.928 ***</td>
<td>2.815 ***</td>
<td>2.997 ***</td>
</tr>
<tr>
<td>Know How Information Obtained</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>2.333 ***</td>
<td>2.341 ***</td>
<td>2.329 ***</td>
</tr>
<tr>
<td>Length of Time Information Misused</td>
<td>0.856 *</td>
<td>0.864 *</td>
<td>0.853 *</td>
</tr>
<tr>
<td>Made Aware by Financial Institution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>0.650 **</td>
<td>0.662 *</td>
<td>0.660 *</td>
</tr>
<tr>
<td>Reported to Financial Institution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>1.002</td>
<td>0.978</td>
<td>0.979</td>
</tr>
<tr>
<td>Reported to Credit Bureau</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>4.287 ***</td>
<td>4.249 ***</td>
<td>4.225 ***</td>
</tr>
<tr>
<td>Age</td>
<td>1.003</td>
<td>1.003</td>
<td>1.003</td>
</tr>
<tr>
<td>Income</td>
<td>0.986</td>
<td>0.982</td>
<td>0.984</td>
</tr>
<tr>
<td>Education</td>
<td>0.992</td>
<td>0.993</td>
<td>0.995</td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td>0.816</td>
<td>0.826</td>
<td>0.813</td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Black</td>
<td>1.210</td>
<td>1.229</td>
<td>1.188</td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td>0.975</td>
<td>1.017</td>
<td>0.977</td>
</tr>
<tr>
<td></td>
<td>Model 6</td>
<td>Model 7</td>
<td>Model 8</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Other</td>
<td>0.984</td>
<td>1.013</td>
<td>0.970</td>
</tr>
<tr>
<td>Marital Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmarried</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Married</td>
<td>0.937</td>
<td>0.974</td>
<td>0.946</td>
</tr>
<tr>
<td>Region</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Northeast</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Midwest</td>
<td>1.825 *</td>
<td>1.871 *</td>
<td>1.881 *</td>
</tr>
<tr>
<td>South</td>
<td>1.811 *</td>
<td>1.828 *</td>
<td>1.849 *</td>
</tr>
<tr>
<td>West</td>
<td>1.194</td>
<td>1.213</td>
<td>1.208</td>
</tr>
<tr>
<td>Pseudo R²</td>
<td>0.226</td>
<td>0.228</td>
<td>0.229</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001

Table 6-6: Logistic regression predicting identity theft victims reporting to financial institutions (n = 5,753)
<table>
<thead>
<tr>
<th></th>
<th>Model 6</th>
<th>Model 7</th>
<th>Model 8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Income</strong></td>
<td>1.007</td>
<td>1.008</td>
<td>1.008</td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td>0.921</td>
<td>0.919</td>
<td>0.919</td>
</tr>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Female</td>
<td>0.927</td>
<td>0.926</td>
<td>0.929</td>
</tr>
<tr>
<td><strong>Race/Ethnicity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Black</td>
<td>0.877</td>
<td>0.872</td>
<td>0.875</td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td>0.985</td>
<td>0.980</td>
<td>0.986</td>
</tr>
<tr>
<td>Other</td>
<td>1.190</td>
<td>1.189</td>
<td>1.197</td>
</tr>
<tr>
<td><strong>Marital Status</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmarried</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Married</td>
<td>0.935</td>
<td>0.926</td>
<td>0.930</td>
</tr>
<tr>
<td><strong>Region</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeast</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Midwest</td>
<td>0.695</td>
<td>0.692</td>
<td>0.697</td>
</tr>
<tr>
<td>South</td>
<td>0.612 *</td>
<td>0.611 *</td>
<td>0.986</td>
</tr>
<tr>
<td>West</td>
<td>0.694</td>
<td>0.689</td>
<td>1.197</td>
</tr>
<tr>
<td><strong>Pseudo R²</strong></td>
<td>0.074</td>
<td>0.074</td>
<td>0.074</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001

Table 6-8: Logistic regression predicting identity theft victims reporting to credit bureaus (n = 5,753)
<table>
<thead>
<tr>
<th></th>
<th>No</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>1.159</td>
<td>1.187</td>
</tr>
<tr>
<td>Reported to Law Enforcement</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>4.279 ***</td>
<td>4.145 ***</td>
</tr>
<tr>
<td>Reported to Financial Institution</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>0.666</td>
<td>0.651</td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td>1.001</td>
<td>1.001</td>
</tr>
<tr>
<td>Income</td>
<td></td>
<td>1.007</td>
<td>1.004</td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td>1.002</td>
<td>1.004</td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Male</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female</td>
<td></td>
<td>0.946</td>
<td>0.948</td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Black</td>
<td></td>
<td>1.798 **</td>
<td>1.868 **</td>
</tr>
<tr>
<td>Hispanic/Latinx</td>
<td></td>
<td>0.985</td>
<td>1.016</td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td>0.976</td>
<td>1.007</td>
</tr>
<tr>
<td>Marital Status</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unmarried</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Married</td>
<td></td>
<td>1.037</td>
<td>1.076</td>
</tr>
<tr>
<td>Region</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Northeast</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Midwest</td>
<td></td>
<td>0.785</td>
<td>0.806</td>
</tr>
<tr>
<td>South</td>
<td></td>
<td>0.694</td>
<td>0.695</td>
</tr>
<tr>
<td>West</td>
<td></td>
<td>0.867</td>
<td>0.889</td>
</tr>
<tr>
<td>Pseudo R²</td>
<td></td>
<td>0.120</td>
<td>0.120</td>
</tr>
</tbody>
</table>

Notes: * p < 0.05; ** p < 0.01; *** p < 0.001