EDITORS' INTRODUCTION

by

Megan M. McNally
School of Criminal Justice
Rutgers University, Newark

Graeme R. Newman
School of Criminal Justice
University at Albany

Identity theft has existed for centuries, but the opportunities for its commission have evolved over time as a function of modernization. While concern for the problem has mounted steadily since the dawn of the information age, it first began to crystallize during the 1990s. Despite the sheer amount of attention this issue has received over the past decade, especially with regard to the steps that individuals should take to prevent their own victimization, there has been a glaring lack of scholarly attention as a whole – an omission that this volume of *Crime Prevention Studies* attempts to redress. In order to contextualize what each contributing author adds to this field, however, it is first necessary to provide a brief background on the issue of identity theft.[1]

The Definition of Identity Theft

Although there has never been a consensus with regard to what identity theft is, this concept generally refers to an instance in which an individual's personal information is used by another to facilitate an act of fraud. The terms *identity theft* and *identity fraud* are often used interchangeably, as

Crime Prevention Studies, volume 23 (2008), pp. 1–8.

they are in the chapters in this volume, but they have also been viewed as separate yet related offense categories. The primary reasons for this are twofold. Historically, *identity fraud* was viewed as being committed against the collective bodies (e.g., governments, financial institutions) that received fraudulent personal information rather than against the people who were fraudulently identified by that information. The term *identity theft*, which did not appear until the late 1980s,[2] was initially used to distinguish individual victims (identity theft) from collective victims (identity fraud) – both of whom were harmed by the same set of criminal activities. More recently, these terms have been applied in a different manner to separate the act of acquiring an individual's personal information (identity theft) from the act of misusing that information (identity fraud); however, since obtaining someone's personal information (e.g., social security number, credit card account number) is a necessary condition for its misuse, many tend to call this combined act *identity theft*. The chapters in this volume therefore deal with both the acquisition (theft) and illicit use (fraud) of identity information.

The misuse of an individual's personal information can also occur in one of two basic ways. Offenders can either access an individual's existing accounts or use another's personal information to open new accounts and/or aid in the commission of other types of fraud. The bulk of identity theft consists of instances in which a victim's personal accounts (i.e., resulting from contracts that s/he has willingly and knowingly entered into, such as credit card accounts, checking or savings accounts, and insurance policies) are compromised by an offending party who has access to pertinent information. The most threatening form of identity theft, sometimes known as "true-name" fraud, occurs when an offender literally assumes another individual's identity to lead a life parallel to the victim's. For example, such offenders can initiate contracts for new accounts of various types, and/or apply for employment, housing and government benefits or provide authorities with their "new" name to escape punishment and avoid detection. Since victims may remain unaware of these activities for extended periods of time, there are often severe consequences associated with this form of identity theft victimization. Although it has sometimes been argued that the term *identity theft* should be reserved for the activities involved in true-name fraud, while the term *identity fraud* should be used for offenses that affect a victim's existing personal accounts, the contributions in this volume are intended to enhance the understanding of identity theft in all of its forms.

The Extent of Identity Theft

It is frequently acknowledged that the present-day specter of identity theft comprises various acts that have long been criminal in the eyes of American law. First recognized as a separate offense by Arizona in 1996, however, identity theft had been criminalized in some form by 2005 within every U.S. state and the District of Columbia, and under federal law. As directed by the Identity Theft and Assumption Deterrence Act of 1998 (Public Law 105-318), the Federal Trade Commission (FTC) began to collect complaint data and provide identity theft information to the public in 1999 through its newly created Identity Theft Clearinghouse (ITC). The ITC, which is currently the only centralized repository for identity theft complaints in the U.S., has since collected over 1 million reports, ranging from a low of 31,117 in 2000 to a high of 255,613 in 2005. These figures steadily increased between 2000 and 2005, but the last published figure for 2006 (246,035) may represent either the beginning of a decline or a leveling off in reporting given its similarity to the figure reported for 2004 (246,882).[3]

The first nationally representative study of this phenomenon, conducted in 2003 on behalf of the FTC (Synovate, 2003), concluded that slightly more than 27 million U.S. adults had been victimized by some form of identity theft during the five-year period between March/April 1998 and March/April 2003. This survey has since been replicated annually by an independent research firm – Javelin Strategy & Research – which has consistently reported a decrease in identity theft victimization over the past few years: 10.1 million U.S. adults in 2003, 9.3 million in 2004, 8.9 million in 2005, 8.4 million in 2006, and 8.1 million in 2007 (Javelin Strategy & Research, 2008).[4]

The National Crime Victimization Survey (NCVS), like the FTC and Javelin studies, also obtains data from a representative sample of U.S. residents. Identity theft questions were recently added to the NCVS, but the results so far have been published separately from its overall findings on national crime victimization; as a result, the relationship between identity theft and the other forms of crime measured by the NCVS is unclear. According to its findings, however, 3.1% of all U.S. households (3.5 million) were victimized by identity theft during a 6-month period in 2004 (Baum, 2006) and 5.5% of all U.S. households (6.4 million) were victimized by identity theft between January and December 2005 (Baum, 2007). It is, nevertheless, difficult to compare these estimates with the findings from the FTC and Javelin victimization surveys, first because of the difference

in measurement units (i.e., households in the NCVS as opposed to individuals in the other two surveys), and second because the 2004 estimate from the NCVS is based on six months' worth of data, rather than one full year.

Results from all three of these victim surveys must be treated with some caution since each measures identity theft victimizations that both are, and are not, reported to the police. In comparison with other types of offending, identity theft victimization reporting patterns are complicated by the fact that these victims often need to contact a non-law enforcement agency for help (e.g., a credit bureau, or the company that issued an account); thus, many victims are able to resolve the issue without having to involve the police. As a result, victimization surveys such as those performed by Javelin and the NCVS represent the uppermost limit of identity theft victimization in the U.S., while the Uniform Crime Reports will reveal the lowest total once police reporting procedures have been standardized. Much of what we currently know about identity theft, however, currently comes from information provided by the victims of this offense – whether this be through a victimization survey or as a result of their request for assistance to various agencies such as the FTC's Identity Theft Clearinghouse.

The Commission of Identity Theft

Although valuable, victim reports are often incomplete with regard to the processes or methods involved in their victimization. Approximately half of all victims, for example, report being aware of how their personal information was obtained. While the majority of these victims report that the information used to commit identity theft was obtained through some type of non-technology-based method (e.g., through a lost/stolen wallet or mail, or by culling through their garbage), the large number of victims who are unaware of how their information was initially obtained leaves much room for speculation about whether technology-based methods were employed (e.g., computers, the Internet). A minority of victims (approximately 25%) also reports knowing who misused their information, but certain categories of offenders (e.g., friends, family members, acquaintances) may be disproportionately over-reported by victims due to the physical and psychological proximity inherent to these types of relationships. The large percentage of offenders who are unknown to their victims has sometimes been interpreted to show that anonymous technology-based methods were used to commit these offenses, but there is not enough evidence to support or refute this view at the present time.

While definitive answers regarding the role of technology in either the acquisition or misuse of personal information are not currently available, it is clear that the contemporary problem of identity theft has been fueled by changes in the ways that personal information is used, stored and transmitted within modern societies. Other factors, such as an increasing reliance on credit and the usurpation of the social security number in America as a primary means for identification, have also converged to help form the foundation upon which identity theft can be accomplished. Although the contributions in this volume only touch upon the complex underpinnings of this collective problem, each is an essential first step toward understanding identity theft more completely and responding more effectively in order to prevent its occurrence.

THE CONTENTS OF THIS VOLUME

This volume of *Crime Prevention Studies* houses a mix of chapters that explore current theory, research and practice regarding the issue of identity theft. The first two chapters are theoretical in scope. Graeme Newman begins with an overview of the opportunity perspective and its application to the study of identity theft. His discussion explores the allure and ease of this offense, with a particular focus on the role of technology in the creation of opportunities for the acquisition and misuse of personal information. This chapter also lays out the foundations of situational crime prevention (SCP) – a common thread running through several of the contributions. Next, Megan McNally examines the meaning and mechanics of identity theft through use of the "script" approach (Cornish, 1994). Her analysis focuses on deconstructing this phenomenon in order to draft a conceptual map of the topic and to identify the opportunities available for research and prevention. Both of these chapters also provide more detailed background information, which serves to flesh out some of the issues mentioned above in this introduction.

The next two contributions present the results of different types of research projects. The chapter by Henry Pontell, Gregory Brown and Anastasia Tosouni outlines new findings from victimization data collected by the Identity Theft Resource Center – an independent non-profit agency devoted to helping victims of this offense and providing information to the public. This contribution is an important example of creating new opportunities for research in order to guide prevention. Their discussion further highlights the ongoing imbalance within popular discourse between

the need for individuals to protect themselves against identity theft and the need for industry members to prevent its occurrence on their behalf. The chapter by Pontell et al. also shows how victimization data can be used to structure future interventions. Next, in one of the few studies of its kind, the chapter by Heith Copes and Lynne Vieraitis explores the commission of identity theft from the offender's perspective. Their findings on the motivations, strategies and skills of identity thieves are used to suggest areas where SCP techniques might be successful in reducing the incidence of identity theft.

Bridging the gap between research and practice is Michael Levi's account of the evolution of identity fraud in the United Kingdom and the programs that have been designed to combat it. This chapter illustrates the international aspects of identity theft, and underscores the similarities and differences between the experiences of the U.K. and the U.S. Levi's analysis further describes the struggle to effect change in the area of plastic card fraud, and emphasizes the universality of some fraud prevention methods. In the next chapter, Russell Smith presents a framework for evaluating preventative interventions related to the challenges of identification. Particular attention is given to the costs and benefits of document-based systems, biometric technologies and identity cards. His discussion also underlines the need to exercise rational choice in the selection of prevention measures, guided by sound research and a consideration of their potential consequences.

The final two chapters focus on understanding how the 25 techniques of situational crime prevention (Cornish and Clarke, 2003) can be used to address the problems underlying identity theft. Sara Berg explores how information technology (IT) can be used in the fight against identity theft. The utility of this approach is demonstrated through the application of eight SCP techniques, using a range of examples from individual to industry prevention. Her discussion also considers the Achilles' heel of technology – human error – and what this might ultimately mean for the effectiveness and future of IT. Finally, Robert Willison examines the use of SCP in the context of information systems security, with a particular emphasis on the "insider" threat posed by employee computer crime. In particular, Willison integrates SCP techniques with the use of "offense scripts" (Cornish, 1994) in order to show how these approaches can work together to strengthen the practices associated with information security, and thereby protect the sensitive personal information that can be used for committing identity theft.

Although the contributions in this volume originate from somewhat different perspectives, all supply something new to our knowledge of identity theft. Several common issues (in addition to SCP) are also addressed throughout the chapters, including definitions, measurement, the scarcity of data, the role of technology, and the importance of cooperation, just to name a few. When read individually, each chapter offers a glimpse into the world of identity theft. When read as a whole, however, this volume captures the diverse dimensions of this topic and the commitment of its contributing authors to understanding identity theft and preventing its occurrence. It is hoped that these pages will inspire others to ask additional questions about what identity theft is and how we should respond to it.

Address correspondence to: MeganM.McNally@gmail.com

NOTES

1. The overview in this chapter is largely based upon the research conducted by Newman and McNally (2005) and McNally (2008), which focused on the development of this issue in the U.S. While three of the chapters in this volume were written by our international compatriots, it is not possible to provide a global history within this introduction; indeed, nothing of this nature currently exists. Many of the issues discussed nevertheless apply in varying degrees to the experiences of other countries.
2. The first-known published use of this term is from a Florida newspaper (Billington, 1989), although earlier records may exist. See McNally (2008) for further information on the history of identity theft and related terminology.
3. These figures were obtained from the annual reports published by the Federal Trade Commission (2007, 2003). The Identity Theft Clearinghouse continually receives data and updates its statistics from previous years within each new annual report, so these numbers are the most recent available.
4. Javelin specifically uses the term *identity fraud* to describe its research, even though it continues the *identity theft* research started by the FTC.

The FTC also recently commissioned a second study (Synovate, 2007), which concluded that 8.3 million U.S. adults had been victimized by some form of identity theft in 2005. The disparity between the figures reported by Javelin (8.9 million) and the FTC (8.3 million) for this year is likely the result of methodological differences. Another figure commonly reported from the original FTC study (Synovate, 2003) is that 9.91 million U.S. adults were victimized during a one-year period ending in March/April 2003. Javelin later reported that 10.1 million U.S. adults had been victimized during 2003, which is attributable to their collection of additional data through the end of that year.

REFERENCES

Baum, K. (2006). *Identity theft, 2004*. Washington, DC: U.S. Bureau of Justice Statistics.

Baum, K. (2007). *Identity theft, 2005*. Washington, DC: U.S. Bureau of Justice Statistics.

Billington, M. (1989, July 6). "Identity theft besmirches victims' records." *Sun-Sentinel*, p. 1B.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. In R.V. Clarke (ed.), *Crime Prevention Studies*, vol. 3, pp. 151-196. Monsey, NY: Criminal Justice Press.

Cornish, D. and R. Clarke (2003). "Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention." In M. Smith and D. Cornish (eds.), *Theory for Practice in Situational Crime Prevention*. (Crime Prevention Studies, vol. 16, pp. 41-96.) Monsey, NY: Criminal Justice Press.

Federal Trade Commission (2003). *National and state trends in fraud & identity theft, January – December 2002*. Washington, DC.

Federal Trade Commission (2007). *Consumer fraud and identity theft complaint data, January – December 2006*. Washington, DC.

Javelin Strategy & Research (2008). *2008 identity fraud survey report: Identity fraud continues to decline, but criminals more effective at using all channels.* Pleasanton, CA.

McNally, M. M. (2008). *Trial by circumstance: Is identity theft a modern-day moral panic?* Unpublished Ph.D. dissertation, Rutgers University.

Newman, G.R. and M.M. McNally (2005). *Identity theft literature review*. Unpublished report prepared for the U.S. National Institute of Justice.

Synovate (2003). *Federal Trade Commission – Identity theft survey report*. McLean, VA.

Synovate (2007). *Federal Trade Commission – 2006 identity theft survey report*. McLean, VA.