Journal of Criminal Law and Criminology

Volume 94
Issue 1 *Fall*

Article 5

Fall 2003

It's Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft

Michael W. Perl

0091-4169/03/9401-0169
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY
Copyright © 2003 by Northwestern University, School of Law
Vol. 94, No. 1
Printed in U.S.A.

IT'S NOT ALWAYS ABOUT THE MONEY: WHY THE STATE IDENTITY THEFT LAWS FAIL TO ADEQUATELY ADDRESS CRIMINAL RECORD IDENTITY THEFT

MICHAEL W. PERL*

I. INTRODUCTION

In October of 1995, Joshua Sours received a letter from Kohl's department store stating that "he owed money to the store in restitution for theft."[1] In fact, Sours's criminal record showed convictions for retail theft and possession of marijuana.[2] The problem was that Sours did not commit these offenses, was never arrested, never appeared in court, and never pled guilty to the offenses.[3]

So what happened to Joshua Sours? Upon receiving the letter from Kohl's, Sours informed police authorities that something was wrong.[4] A subsequent investigation revealed that when the suspect of the Kohl's theft was arrested, he identified himself as Joshua Sours, attended one hearing, pled guilty to the charges, was sentenced to a day in jail, and was then released by authorities.[5] When Sours learned of these past events, a "quick look at the police photo" clarified what had happened.[6] Sours realized that

* J.D. Candidate, 2004, Northwestern University School of Law; B.S., Finance, 2000, Yeshiva University. I thank my wife, Tova, and my daughters, Julie and Ariella, for their constant devotion, support, and patience that were necessary to write, edit, and publish this Comment. I also thank Clifford Zimmerman, Clinical Associate Professor of Law, Northwestern University School of Law, and Sophia Lopez, Supervisor of Consumer Fraud Division, Cook County State's Attorney's Office for reviewing this article and providing me with helpful comments and suggestions.

[1] Phil Borchmann, *Wrong Man Convicted, Cops Admit*, CHI. TRIB. (McHenry County), Oct. 20, 1995, at 1.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

the true perpetrator of the crimes was actually a high school friend, using Sours's identity to protect himself from obtaining a tainted criminal record.[7]

Sours was a victim of criminal record identity theft,[8] a form of identity theft whose popularity continues to rise throughout the country.[9] Criminal record identity theft occurs when the identity thief obtains a victim's personal information[10] and then commits crimes, traffic violations, or other illegal activities while acting as the victim.[11] Instead of providing law enforcement with her own personal information, the identity thief provides the victim's personal information in order for the identity thief to avoid criminal convictions and legal sanctions in her own name.[12] This Comment will address this specific form of identity theft in further detail.

---

[7] *Id.*

[8] This form of identity theft is sometimes referred to as "criminal identity theft." *See, e.g.*, LINDA FOLEY ET AL., FACT SHEET 17(G): CRIMINAL IDENTITY THEFT, WHAT TO DO IF IT HAPPENS TO YOU, (rev. May 2002), *available at* http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm. However, "criminal record identity theft" is a more accurate name for this form of identity theft. Most types of identity theft are criminal in nature, so any form of identity theft could conceivably be considered "criminal identity theft." See *infra* Part III for a discussion of the laws making identity theft a crime. Therefore, for purposes of this Comment, I will refer to this form of identity theft as "criminal record identity theft."

[9] Beth Givens, *Identity Theft: The Growing Problem of Wrongful Criminal Records*, Presentation at the SEARCH National Conference on Privacy, Technology and Criminal Justice Information in Washington, D.C. (June 1, 2000), *available at* http://www.privacyrights.org/ar/wcr.htm; *see also* Allison Klein, *Stolen Name, Sullied Record, Lingering Harm*, BALT. SUN, Dec. 26, 2002, at 1A ("[Criminal record identity theft is] so common in Baltimore that victims have recently been overwhelming the prosecutor's office. At least four times a week, a person with a similar problem walks into her office seeking help . . . . Two years ago, she saw about one a week.").

[10] For a discussion of the various ways that an identity thief may obtain a victim's personal information, see *infra* Part II.A.

[11] Givens, *supra* note 9.

[12] The FTC reports that in 2001, "[a]lmost 2% of all [identity theft] victims reported that the thief assumed their identity to evade legal sanctions and criminal records (thus leaving the victim with a wrongful criminal or other legal record) . . . ." IDENTITY THEFT CLEARINGHOUSE, FED. TRADE COMM'N, IDENTITY THEFT COMPLAINT DATA: FIGURES AND TRENDS ON IDENTITY THEFT JANUARY 2001 THROUGH DECEMBER 2001, at 4 (2002), *available at* http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2001.pdf [hereinafter FTC (FIGURES AND TRENDS 2001)]; E-mail from Joanna Crane, Director of Identity Theft, FTC (Nov. 6, 2002, 14:11 EST) (on file with author) (reporting that in 2001 there were 1456 victims of criminal record identity theft who contacted the FTC to report that they were victims). However, there may be many more victims who did not contact the FTC or are unaware that their criminal record is being used by an identity thief. Beth Givens, the director of the Privacy Rights Clearinghouse in California states that one in six victims, or fifteen percent, of victims of financial identity theft reported that they also had erroneous criminal records. Givens, *supra* note 9. It is important to note that the FTC collects data and reports statistics regarding the crime of identity theft. However, the FTC is a civil agency and identity theft is criminal in nature. Thus, while the FTC compiles the statistics regarding

Although identity theft is a crime in almost every state,[13] as well as a federal felony, most state identity theft laws need to be amended to adequately detect, prevent, and prosecute criminal record identity theft because most identity theft prosecutions occur at the state level.[14] This Comment will explore the current state identity theft laws in detail and explain the provisions that are necessary to comprehensively address criminal record identity theft.

Before addressing the identity theft laws in more detail, Part II will provide some general background information about the crime of identity theft. It will explain the specific ways an identity thief obtains a victim's personal information and the various ways in which the thief may use that information, including criminal record purposes. Part III will then examine the current identity theft laws to see if and how these laws address criminal record identity theft. It will explain that although some states recognize criminal record identity theft as a crime, many states treat criminal record and financial identity theft differently in various ways.[15] It will also explain that the current laws fail to adequately address the statute of limitations issue as well as "reverse criminal record identity theft," a specific form of criminal record identity theft.[16] Finally, Part IV will explore two potential ways that the problem of criminal record identity theft may be better controlled.[17]

---

identity theft, the FTC does not prosecute identity thieves. Telephone Interview with Sophia Lopez, Supervisor of Consumer Fraud Division, Cook County State's Attorney's Office (Aug. 18, 2003) (notes on file with author).

[13] For a discussion of the federal and state identity theft laws, see *infra* Part III.

[14] *See infra* note 88 and accompanying text (explaining that most identity theft prosecutions occur at the state level because federal prosecutors generally do not prosecute identity thieves unless a sizable amount of money is involved and because state judges have more discretion than federal judges when imposing penalties because federal judges are subject to the Federal Sentencing Guidelines).

[15] *See infra* Part III.B (explaining that some states differentiate financial and criminal record identity theft with respect to gradation of penalty, repeat offenders, and assisting the victims).

[16] *See infra* Part III.C; *see also infra* notes 63-66 and accompanying text (explaining what constitutes reverse criminal identity theft).

[17] *See infra* Part IV.A-B (suggesting to create a link between the intermediary parties between the victim and thief and to increase the use of biometric data).

II. BACKGROUND

Identity theft is the fastest growing crime in the United States.[18] Due to the widespread growth of identity theft, in 1999 the Federal Trade Commission ("FTC") began collecting consumer complaints[19] related to identity theft in the Identity Theft Clearinghouse.[20] Between 2000 and 2001 alone, both the numbers of inquiries to the FTC related to identity theft and the reported identity theft victims nearly tripled.[21] Moreover, the FTC reports that the number of identity theft claims more than doubled between 2001 and 2002.[22] Thus, with the number of incidents of identity theft reported to the FTC between 2000 and 2002 increasing from nearly 31,000 to about 162,000, today there are more than five times as many reported incidents of identity theft as there were only three years ago.[23]

---

[18] S. 1742, 107th Cong. § 2 (2001); *see also* Sandra Block, *States Pass Laws to Protect Identity*, USA TODAY, July 14, 2003, at 1B; Brigid Schulte, *County Police Take a Bite Out of Fraud; Small Unit Faces Growing Caseload*, WASH. POST, May 22, 2003, at T18.

[19] The FTC processes reports related to identity theft. Of these reports, the majority are victims reporting that they have been victimized, but some reports are simply from consumers concerned about identity theft in general. FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 1. Thus, for purposes of this Comment, an "inquiry" or "report" to the FTC may or may not be an actual victim of identity theft; whereas a "claim," "incident," or "victim" refers to an actual victim of identity theft, not a mere inquiry.

[20] *Id.*

[21] The FTC reported that it processed more than 40,000 inquiries from consumers and identity theft victims in 2000. IDENTITY THEFT CLEARINGHOUSE, FED. TRADE COMM'N, IDENTITY THEFT COMPLAINT DATA: FIGURES AND TRENDS ON IDENTITY THEFT JANUARY 2000 THROUGH DECEMBER 2000, at 1 (2001), *available at* http://www.ftc.gov/bcp/workshops/idtheft/trends-update_2000.pdf [hereinafter FTC (FIGURES AND TRENDS 2000)]. Of those inquiries, sixty-nine percent were actual victims reporting one or more types of identity theft incidents. *Id.* Although this indicates that there were 27,600 reported identity theft victims in 2000, the FTC also reports that there were 31,103 reported identity theft victims in 2000. IDENTITY THEFT CLEARINGHOUSE, FED. TRADE COMM'N, IDENTITY THEFT VICTIM COMPLAINT DATA: FIGURES AND TRENDS ON IDENTITY THEFT JANUARY 2000 THROUGH DECEMBER 2000, at 1; *see also* Noel C. Paul, *Identity Heist!*, CHRISTIAN SCI. MONITOR, Feb. 19, 2002, at 17 (stating that FTC reported 31,103 Americans who were victims of identity theft in 2000). Thus, for purposes of this section, I will use 31,000 because that is the actual number reported by the FTC. In 2001, the number of inquiries to the FTC increased to 117,210. FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 1. Of those inquiries, 86,168, or seventy-four percent, were victims reporting their personal episodes of identity theft. *Id.*

[22] Jennifer 8. Lee, *Identity Theft Complaints Double in '02, Continuing to Rise*, N.Y. TIMES, Jan. 23, 2003, at A18. However, the FTC estimates that there are more than 700,000 identity theft victims each year. Associated Press, *Identity Theft No. 1 in Consumer Fraud*, CHI. TRIB., Jan. 23, 2002, at B2. Thus, only a fraction of the identity theft incidences are being reported to the FTC each year.

[23] *See supra* notes 21-22 and accompanying text.

Identity theft is "the theft of identity information such as a name, date of birth, Social Security Number, . . . credit card number,"[24] or any other personal identification information in order to obtain "loans in the victim's name, steal money from the victim's bank accounts, illegally secure professional licenses, drivers licenses, and birth certificates,"[25] or other unauthorized use of the victim's personal information for financial or other activity.[26]

This section will discuss how identity thieves obtain the necessary information in order to assume a victim's identity and the various ways in which identity thieves exploit the victim's personal information for their own personal benefit.

A. METHODS BY WHICH IDENTITY THIEVES OBTAIN VICTIMS' PERSONAL INFORMATION

Identity thieves use various techniques to obtain personal information ranging from mundane activities to high-tech inventions. The classic method involves searching the victim's garbage to find old credit card bills, bank statements, utility bills, phone bills, or any other document that has a name, address, or account information.[27] Identity thieves may rummage through a victim's mail[28] or call a potential victim's home, acting as a banker who is calling to "verify" credit card information.[29] Other techniques include looking over someone's shoulder in the checkout line at a supermarket or other store in order to learn the person's name and Social

---

[24] Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1423 (2001).

[25] Martha A. Sabol, *The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?*, 11 LOY. CONSUMER L. REV. 165, 166 (1999).

[26] See *infra* Part III for a discussion of specific state and federal identity theft laws.

[27] IDENTITY THEFT CLEARINGHOUSE, FED. TRADE COMM'N, ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME 3 (2002), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf [hereinafter FTC (WHEN BAD THINGS HAPPEN)].

[28] *Id.*; Hoar, *supra* note 24, at 1440; FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 3; Paul, *supra* note 21, at 17. Some thieves focus on those who send out their mail in curb side mailboxes. Others prefer incoming mail, especially for pre-approved credit card applications, which are "particularly mouth watering targets for theft." Paul, *supra* note 21, at 17. A thief can fill out the application and then change the address on the account before a billing cycle begins. This provides an easy way for an identity thief to obtain a credit card in the victim's name. Furthermore, because the victim is not necessarily expecting such an application to arrive in the mail, the victim would be unaware that the pre-approved application was even taken.

[29] Paul, *supra* note 21, at 17.

Security Number, which is often sufficient to obtain personal identification under the victim's name.[30]

Some identity thieves use more advanced practices to obtain the victim's personal information. Cashiers may use a "swiper,"[31] a small device that allows the one swiping a credit card to obtain and store all of the cardholder's personal information.[32] The personal information can then be downloaded or scanned directly into a false credit card.[33]

The advancement of computer technology and the development of the Internet have provided identity thieves with more options to obtain the necessary information to carry out their crime.[34] Identity thieves may be able to obtain a victim's personal information by hacking into a database, personal computer, or a company's computer system.[35] The Internet, therefore, allows a potential identity thief to obtain a victim's personal information from her home, office, public library, hotel room, or any other location with Internet accessibility. Such easy access obviates the need for an identity thief to rummage through a victim's garbage or mail, follow a victim to a supermarket, or any other conventional method of obtaining a victim's personal information.[36] Moreover, the Internet allows identity thieves to seek out victims from virtually anywhere in the world.[37] Finally, the identity thief may carry out her crime via the Internet, regardless of how the victim's personal information is obtained.[38]

---

[30] *Id.* The thief can then complete the victim's personal profile by looking up the victim on-line or in a phone book to obtain the victim's address. *Id.* Having a name, Social Security Number, and address is usually adequate to request a copy of the person's birth certificate over the phone, or even to obtain a driver's license in the victim's name. *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.* This device is not set up by the merchant to assure safety. Rather, the device is used by the sales clerk to steal someone's personal identification information.

[34] There is probably sufficient information to write an entire Comment on the impact of the Internet on the crime of identity theft. While this Comment may touch on some of those aspects, its focus will not be on the Internet. For an in depth analysis of crimes in cyberspace, see Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001).

[35] *See, e.g.*, Lee, *supra* note 22, at A18.

[36] *See id.* (quoting William Crane, Assistant Director of the National White Collar Crime Center: "The Internet is facilitating non-person-to-person transactions on a global scale.").

[37] While an identity thief can conceivably travel to any city, state, or country to search through a victim's garbage or mail, realistically, an identity thief would find an easily accessible victim from a relatively nearby location. With the Internet, however, a person living in Chicago is the same click-of-a-mouse away from his next door neighbor, a friend in Milwaukee or New York, or someone living in Israel, China, or Australia. Thus, the Internet broadens the potential pool of victims available for an identity thief to exploit.

[38] Katyal, *supra* note 34, at 1027. The Internet can be a prime place to carry out financial

While the Internet has had a direct impact on the recent proliferation of identity theft,[39] the crime would still be a problem without the Internet.[40] This is because another frequently used method of obtaining victims' personal information is through an "inside job."[41] This occurs when information is obtained by a fellow employee at a place of employment and then is used or given to someone else to carry out an identity theft crime.[42] "Inside jobs" are troubling for two reasons. First, many suggested techniques to avoid becoming a victim of identity theft, which include shredding old bills, bank statements, and pre-approved credit card applications, as well as not carrying around one's Social Security Number in a purse or wallet, will likely be ineffective to protect against an "inside job."[43] Moreover, an "inside job" may provide the identity thief with the identification information of thousands of potential victims, thus creating breeding grounds for mass identity theft to occur.[44]

B. DIFFERENT FORMS OF IDENTITY THEFT

Once an identity thief obtains the personal information of a potential victim, the thief can use that information in various ways. While this Comment will focus on criminal record identity theft, most reported cases of identity theft involve financial motivation.[45] Because criminal record

---

identity theft by registering for credit cards, applying for loans, and making purchases. But because most of these methods involve financial identity theft, they are beyond the scope of this Comment, which focuses on criminal record identity theft.

[39] *Id.* (stating that the Internet has made it easier for identity thieves to carry out their crime); *see also* Lee, *supra* note 22, at A18.

[40] *See infra* notes 41-44 and accompanying text.

[41] Katherine Millett, *Self Preservation*, CHI. TRIB., Aug. 19, 2001, (Magazine), at 12. The FTC refers to an "inside job" as "business record theft." FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 3.

[42] FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 3; *see also* Robert Hanley, *Former H&R Block Manager Accused in Identity-Theft Ring*, N.Y. TIMES, Jan. 3, 2003, at B2 (stating that an H&R Block employee who had access to personal and financial information of various clients was involved in an identity theft ring in White Plains New York).

[43] *See, e.g.*, Lee, *supra* note 22, at A18 (stating that one suspect in a three-man identity theft ring in New York worked at a software company and was able to call up credit reports to assist in victimizing over 30,000 people).

[44] *See id.*

[45] *See* FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 2-4 (discussing the breakdown of all reported cases of identity theft during 2001); FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 4 (listing eight ways in which an identity thief can use a victim's personal information). Many victims of identity theft report that their personal information has been used for more than one purpose. Therefore, the percentages reported by the FTC correspond to the number of complaints that were filed for each purpose. Meaning, if a victim's

identity theft is only one form of the broader crime of identity theft, a brief look at other types of identity theft is instructive to attain a better understanding of criminal record identity theft.

1. Financial Identity Theft

Financial identity theft occurs when the identity thief uses a victim's personal information to withdraw money from a victim's bank account, open a new bank account,[46] credit card,[47] or other line of credit[48] in the victim's name, or files a bankruptcy petition using the victim's name.[49] With respect to credit lines, the thief generally defaults on the loans and the delinquent account(s) is reported on the victim's credit report.[50] This leaves the victim with both a damaged credit history and the burden of clearing her credit history,[51] an emotionally draining process requiring a great deal of the victim's time, energy, and resources.[52]

---

personal information was used both for financial and criminal record purposes, and both incidents were reported to the FTC, the FTC would report each complaint separately. *See* FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 2 n.1.

[46] FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 2-3 (stating that thirteen percent of complaints related to victims' bank accounts including reports of fraudulent checks, unauthorized withdrawals from an existing account, and new bank accounts that were opened in the victim's name).

[47] *Id.* at 2 (reporting that forty-two percent of victims complained of credit card fraud: twenty-six percent of victims reported that "one or more new credit cards were opened in their name, making this the most commonly reported misuse of victim's information," ten percent of the victims reported unauthorized charges appeared on existing credit cards, while the remaining six percent of victims reporting credit card fraud did not specify whether a new card was opened in the victim's name or if unauthorized charges appeared on existing accounts).

[48] *Id.* at 3 (stating that these include personal, student, business, real estate, or auto loans); *see also* FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 3.

[49] *See, e.g.*, *In re* Riccardo, 248 B.R. 717 (Bankr. S.D.N.Y. 2000). An identity thief may file for bankruptcy in the victim's name, which allows the identity thief to avoid paying for debts that the thief incurred in the name of the victim. FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 4. An individual may seek bankruptcy protection under chapters seven, eleven, or thirteen of the bankruptcy code. While filing any bankruptcy petition can be damaging to one's credit history, using the victim's personal information to file a chapter seven bankruptcy (discharge) has a potentially harsh impact for the victim. One may only obtain a discharge from her debts under chapter seven of the bankruptcy code once every six years. 11 U.S.C. § 727 (a)(8) (2000). Thus, not only will the bankruptcy likely damage the victim's credit rating, but it may prevent the victim from filing her own bankruptcy should she need to do so.

[50] *See* FTC (WHEN BAD THINGS HAPPEN), *supra* note 27, at 4.

[51] Susan Langenhennig, *Identity Theft Can Produce a Nightmare*, THE TIMES-PICAYUNE (N. ORLEANS), July 29, 2001, at 1.

[52] The Identity Theft Resource Center in San Diego reports that a victim of identity theft spends an average of 175 hours per year trying to clear her damaged name. Hiram Soto,

In addition to the burden of clearing her name, a victim may be unaware that she has become a victim of identity theft until weeks, months, or even years after the damage has already been done.[53] For example, a victim may learn that she is being victimized by simple occurrences such as receiving credit card bills from credit cards for which she never applied, noticing items on a credit report or credit card bill for which she is not responsible, or observing that certain bills have missed a billing cycle.[54]

In other cases the victim may become aware that she has been victimized in a more unexpected way. For instance, a victim's application for a new credit card, mortgage, automobile loan, or other line of credit may be denied because her credit history is tainted with delinquencies caused by the identity thief.[55] Only then does the victim realize that her credit report contains credit cards for which she never applied, bills that are long overdue, unfamiliar billing addresses, and inquiries from creditors that she does not recognize.[56]

2. Non-Financial Identity Theft

Although financial reasons are the most common motivation for identity theft,[57] other factors motivate identity theft as well. Thieves may use a victim's personal information for telecommunications and utilities fraud,[58] or to obtain government documents or benefits in the victim's

---

Identity Theft Turns into Growing Problem; Woman Endured Decades of Hassles, SAN DIEGO UNION-TRIB., Feb. 5, 2002, at B2. Clearing a victim's name "involves phone calls and letters to credit agencies, financial institutions, phone companies, police departments and other government agencies." *Id.*

[53] *See* Hoar, *supra* note 24, at 1425-26; *see also* FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 6 (reporting that in 2001 the average time between the first unauthorized use of the victim's personal information and when the victim first realizes that she has become a victim of identity theft is 12.3 months). However, most victims (sixty-nine percent) stated that they became aware that they were victims of identity theft within six months of the first unauthorized use. *Id.* In fact, of that amount, forty-four percent discovered that they had become a victim of identity theft within one month of the first unauthorized use. *Id.* But sixteen percent of victims remained unaware that they had been a victim of identity theft for more than two years. *Id.*

[54] *See* FED. TRADE COMM'N, IDENTITY CRISIS . . . WHAT TO DO IF YOUR IDENTITY IS STOLEN (2000) at 1, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/ idenalrt.pdf.

[55] *See* Hoar, *supra* note 24, at 1425.

[56] *Id.*

[57] *See supra* note 45 and accompanying text.

[58] FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 2. Twenty percent of victims reporting to the FTC in 2001 reported that the thief "obtained unauthorized telecommunications or utility equipment or services in their name." *Id.* The most common of these complaints was that the thief obtained new wireless phone services and equipment in the victim's name. *Id.* Others reported that new phone services were setup in their

name.[59] Such documents could be used for various purposes including unlawful entry to the country[60] and to carry out terrorist attacks.[61] In addition, nine percent of those who reported that they were victims of identity theft in 2001 indicated that their personal information was used by the identity thief to obtain a job.[62]

Using a victim's identity to obtain a job is particularly interesting for this Comment because in some cases it may constitute "reverse record identity theft,"[63] a subset of criminal record identity theft.[64] In a classic case of criminal record identity theft,[65] the thief obtains and uses the victim's personal information in order to avoid traffic violations or criminal convictions from appearing in her own name, but simultaneously causes the

---

homes, new phone equipment was purchased in their names, or that other utility services including electric and cable television services were established in the victim's name. *Id.*

[59] *Id.* at 3 (stating that three percent of victims reported that identity thieves used a driver's license in the victim's name and a small percentage of victims reported that the identity thief used a social security card or some other official document in the victim's name).

[60] *See* Stephanie Rubec, *Is ID Debate in the Cards?; Immigration Minister Pushes for Discussion*, TORONTO SUN, Feb. 7, 2003, at 51 (stating that an ID card containing a person's biometric data will help crack down on identity theft and assist with controlling borders).

[61] *See* Norman A. Willox Jr., *Knowledge-Based ID System Fights Fraud*, DETROIT NEWS, Jan. 12, 2003, at 11A (noting that the September 11th hijackers used false identification documents to obtain airplane tickets to carryout the terrorist attacks).

[62] FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 3. Although the FTC did not specifically explain how an identity thief does this, frequently the identity thief has a criminal record, and a background check by an employer would likely reveal the identity thief's criminal history. *See, e.g.*, Michele McNiel Solida, *Governor: Pensions Not at Risk; Because of Cursory ID Check, State May have Hired Felon Even if He Hadn't Lied for Job*, INDIANAPOLIS STAR, Aug. 16, 2002, at 1A. Therefore, the identity thief uses the victim's name, Social Security Number, and other personal information, so when the employer conducts a background check, the clean record of the victim will appear as if it belongs to the identity thief. That is not to say all identity thieves who use a victim's identity to obtain a job do so to avoid discovery of a criminal record. For example, the identity thief may be an illegal immigrant who is unable to get a job on her own. Therefore, using a victim's identity to obtain a job may or may not always be a form of criminal record identity theft.

[63] "Reverse criminal record identity theft" is not a legal term. Rather, it is a term that I use to describe a situation which is the "reverse" of classic criminal record identity theft. The irony of reverse criminal record identity theft in the context of employment is that often victims of classic criminal record identity theft find out that they have been victimized when they attempt to obtain employment and are denied employment because the employer discovers that the victim has a criminal record. In this case, the identity thief is using the victim's clean record to avoid revelation of her own criminal record in order to obtain employment himself.

[64] See *infra* notes 190-202 and accompanying text for a discussion of how the state identity theft laws generally fail to address reverse criminal record identity theft.

[65] See *infra* notes 66-70 and accompanying text for a more detailed explanation of criminal record identity theft.

innocent victim to appear as a criminal. However, in reverse criminal record identity theft, the thief is already a convicted criminal; the thief uses the victim's identity in order to prevent someone else from detecting the thief's criminal record. This form of identity theft arises in the employment context because convicted criminals often have difficulties passing a background check to secure employment.[66] Using a victim's clean record may help a convicted criminal pass such a background check without her own convictions ever being discovered. Thus, in the classic case of criminal record identity theft, the identity theft causes the innocent to erroneously appear as a criminal. But in the "reverse" scenario, the identity theft causes the criminal to erroneously appear innocent.

3. Criminal Record Identity Theft

Identity thieves may use the victim's personal information "to evade legal sanctions and criminal records (thus leaving the victim with a wrongful criminal or other legal record)."[67] Similar to financial identity theft, a victim of criminal record identity theft is usually unaware that her identity has been stolen and is being used by the thief.[68] A victim may only become aware of her predicament when she attempts to renew a driver license,[69] reports to a new job,[70] receives a citation notice from a court, phone calls from a collection agency, a notice of an outstanding arrest warrant, is pulled over for a traffic violation and learns that her license has been revoked, or is actually arrested for crimes committed by the identity thief.[71]

Criminal record identity theft has been called "the worst-case scenario of identity theft" because it presents several problems both for law enforcement and for the victims.[72] While the nature of any identity theft

---

[66] FOLEY ET AL., *supra* note 8.

[67] FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 4.

[68] *See, e.g.*, Smith v. Ill. Sec'y of State, No. 01 C 1605, 2002 U.S. Dist. Lexis 1318 (N.D. Ill. Jan. 28, 2002) (regarding innocent motorist who attempted to renew his driver's license, but unbeknownst to him, he had multiple traffic violations on his driving record which resulted in suspension of his license).

[69] *Id.*

[70] *See, e.g.*, Givens, *supra* note 9 (citing Valerie Alvord, *When Dreams Turn Ugly: Stolen Identity Puts Her Budding Career in Handcuffs*, SAN DIEGO UNION-TRIB., Aug. 29, 1999) (where employer's background check revealed felony convictions or arrest warrants listed on the victim's criminal record that victim was unaware of because crimes were committed by the identity thief); *see also* Klein, *supra* note 9, at 1A (stating that victims of criminal record identity theft usually find out that they have been victimized when applying for a job).

[71] FOLEY ET AL., *supra* note 8.

[72] Givens, *supra* note 9.

crime present difficulties for law enforcement and victims, criminal record identity theft presents two unique problems not associated with other forms of identity theft. First, criminal record identity theft allows criminals to stay on the street without being arrested or penalized for their traffic violations or criminal offenses.[73] Second, clearing or correcting an erroneous criminal record can be difficult for victims due to the lack of established procedures[74] and the necessity of a court order under certain circumstances in order to have an erroneous criminal record expunged.[75] Furthermore, even if a victim were to contact the criminal records department where the erroneous criminal record was recorded, the record keepers generally lack authority to change a criminal record.[76] A judge must make the determination that a criminal record is erroneous and decide whether the record should be amended, cleared, or expunged.[77] Thus, the burden is usually on the victim to initiate and follow through with the procedures necessary for having her record cleared or expunged,[78] which often requires countless phone calls, letters, hours, and expenses.[79]

---

[73] This could impact punishments for offenses that carry harsher punishments for repeat offenders. For example, the Secretary of State in Illinois reports that a driver who is convicted of "driving under the influence of alcohol, other drugs and/or intoxicating compounds" will have his driver's license revoked "for a minimum of one year for the first offense, five years for a second offense committed within a 20-year period, 10 years for a third offense and lifetime revocation for a fourth or subsequent offense." ILL. SEC'Y OF ST., CYBER DRIVE ILL., *at* http://www.cyberdriveillinois.com/departments/drivers/faq.html#Suspensions (last visited Mar. 11, 2003). Similarly, the criminal justice system often wastes time and resources pursuing identity theft victims with erroneous arrest warrants or convictions on their records only because of the actions of an identity thief.

[74] Givens, *supra* note 9; FOLEY ET AL., *supra* note 8 ("[T]he responsibility to correct the erroneous data in the various criminal justice computer systems is with the officials working within the criminal justice system. There are no established procedures for clearing one's wrongful criminal record."). Additionally, expunging erroneous convictions incurred in the victim's name does not trigger standard expungement procedures because criminal record identity theft involves a situation where the perpetrator of the crime should have the conviction on her criminal record, but the victim of identity theft wants to have her record cleared. For a thorough overview of expunging criminal records, see Michael D. Mayfield, *Revisiting Expungement: Concealing Information in the Information Age*, 1997 UTAH L. REV. 1057.

[75] *See* Klein, *supra* note 9 (stating that criminal record identity theft can ruin a victim's life). Because of the devastating impact on the victims, the difficulty of having erroneous criminal convictions expunged (felony convictions require a court order), and the difficulty of correcting a record when someone's name is attached to a set of finger prints, the highest Court in Maryland is attempting to devise a system to deal with these difficulties. *Id.*

[76] Telephone Interview with Sophia Lopez, *supra* note 12 (explaining that criminal record divisions just keep records for the courts, but a judge must make a determination that a record should be cleared) (notes on file with author).

[77] *Id.*

[78] The process of having one's criminal record expunged is difficult. Smith v. Ill. Sec'y

Moreover, while credit delinquencies remain on one's credit report for seven years,[80] certain traffic violations or criminal convictions may remain on the offender's record forever.[81] Thus, simply allowing time to pass will be insufficient to cure the problem.[82]

With an understanding of the potential impacts of identity theft in general, and criminal record identity theft in particular, this Comment will now focus on the current laws and procedures in place to address and prevent criminal record identity theft.

III. CURRENT IDENTITY THEFT LAWS

In June 2002, the United States General Accounting Office ("GAO") conducted a survey of ten states[83] to investigate how those states were addressing and managing the problem of identity theft.[84] While the survey is helpful to obtain an overall status of the identity theft laws, consistent with most of the literature on identity theft, the survey primarily focuses on identity theft for financial purposes.[85]

However, a minority of states have provisions in their identity theft laws that unquestionably address criminal record identity theft directly.[86]

---

of State, No. 01 C 1605, 2002 U.S. Dist. LEXIS 1318, at 7 (N.D. Ill. Jan. 28, 2002).

[79] Givens, *supra* note 9; FOLEY ET AL., *supra* note 8; *see also* T. Shawn Taylor, *File this Away: Thieves Can Get You at Work*, CHI. TRIB., Dec. 4, 2002, at C1 (stating that the average identity theft victim spends $800-$1100 and about 175-200 hours clearing her name).

[80] Ronald C. Claiborne, *Credit Reports and the Fair Credit Reporting Act*, 28 J. MARSHALL L. REV. 365, 367 (1995) (citing 15 U.S.C. § 1681c(a)(2)-(6) (1992)).

[81] *See, e.g.*, ILL. SEC'Y OF ST., *supra* note 73 (reporting that in Illinois any alcohol or drug offense remain on a driver's record for the duration of the driver's life).

[82] That is not to say that in a case of financial identity theft simply allowing seven years to pass in order to have the delinquencies lapse is an adequate remedy for the victim. However, in contrast to a victim of financial identity theft where the damage could be for a finite time period, a criminal record identity theft victim could be affected forever.

[83] The survey looked at Arizona, California, Florida, Georgia, Illinois, Michigan, New Jersey, Pennsylvania, Texas, and Wisconsin. The GAO chose these ten states specifically because these states either had the highest number of reported incidences of identity theft or had statutes in place to address identity theft for the longest period of time. U.S. GEN. ACCOUNTING OFFICE, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED (2002) [hereinafter GAO].

[84] *Id.* at 2. The survey states that the increase of identity theft incidences is a "serious problem across the nation," and many state and federal laws have been passed to deal with the crime. *Id.* at 1-2.

[85] The reason for this focus is likely that most of the laws and procedures in place focus on identity theft for financial purposes.

[86] *See, e.g.*, CAL. PENAL CODE §§ 530.5-.8 (West Supp. 2003); MD. CODE ANN., CRIMINAL LAW § 8-301(c) (2002 & Supp. 2003); NEV. REV. STAT. ANN. 205.463(2) (Michie 2001); N.Y. PENAL LAW §§ 190.78(2), 190.79(3), 190.80(3) (Consol. Supp. 2003); N.C.

This section will look at the current identity theft laws to see how criminal record identity theft is addressed by these statutes.[87]

Most identity theft prosecutions occur at the state level pursuant to state law.[88] Moreover, with respect to criminal record identity theft, the majority of law enforcement occurs at the state level because most false criminal records established by identity thieves are for state criminal laws rather than federal laws.[89] Thus, to understand the laws under which most identity theft cases are prosecuted, it is necessary to look at the state identity theft laws.[90]

However, in addition to the state identity theft laws, Congress passed a federal identity theft law in 1998.[91] Although prosecutions under the federal law are less frequent than under state laws, for completeness this

---

GEN. STAT. § 14-113.22 (2001); UTAH CODE ANN. § 76-6-1104 (Supp. 2003); VA. CODE ANN. § 18.2-186.3(D) (Michie Supp. 2003); and WYO. STAT. ANN. § 6-3-901(e) (Michie 2003). These state statutes have provisions that unquestionably address criminal record identity theft. But as will be explained in more detail below, other states have open-ended language that may allow prosecution of criminal record identity theft.

[87] There may be other state statutes under which an identity thief may be prosecuted. For example, an identity thief, through her actions, may violate a state identity theft law as well as a criminal misrepresentation law or a forgery law. Thus, while the actions of an identity thief may qualify as violations of multiple laws, this Comment will focus only on the state identity theft laws.

[88] Telephone Interview with Chris Clapper, Special Agent with Secret Service, Liaison to Federal Trade Commission's Identity Theft Program (Jan. 8, 2003) (notes on file with author). Most identity theft prosecutions occur under state law for two reasons. First, federal prosecutors generally will not take the case unless a sizable amount of money is involved. *Id.* Second, because punishments of federal crimes are subject to the Federal Sentencing Guidelines, the potential punishments for identity thieves are stricter under state law. *Id.* Under state laws the judges have more discretion to impose harsher punishments as opposed to the federal sentencing guidelines, which is more of a formulaic punishment system. *Id.* Thus, in most cases, prosecutors choose to prosecute under state law rather than federal law.

[89] E-mail from Joanna Crane, *supra* note 12 and accompanying text.

[90] States refer to identity theft in different ways. Some states refer to the crime as "identity theft." *See, e.g.*, IOWA CODE ANN. § 715A.8 (West 2003). Other states call the crime "identity fraud." *See, e.g.*, VA. CODE ANN. § 18.2-186.3. Other states refer to the crime more generically as "impersonation" or "unauthorized use of personal identifying information." *See, e.g.*, N.J. STAT. ANN. § 2C:21-17 (West Supp. 2003) ("Impersonation"); WYO. STAT. ANN. § 6-3-901 ("Unauthorized use of personal identifying information"). This is not an exhaustive list of all the different names that states use to refer to the crime of identity theft. However, the substance of the crime is similar from state to state (not including the different provisions that each individual state may include). For purposes of this Comment, I will refer to the crime as "identity theft," which includes the other names of the crime as well.

[91] 18 U.S.C. § 1028(a)(7) (2000).

Comment will briefly look at the federal identity theft law before analyzing the state identity theft laws in detail.

A. FEDERAL IDENTITY THEFT AND ASSUMPTION DETERRENT ACT

In November of 1998, Congress passed the Identity Theft and Assumption Deterrent Act ("ITADA").[92] Under ITADA, it is unlawful if a person "knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[93] Prior to 1998, sections (a)(1) through (a)(6) of ITADA prohibited "the unauthorized use or transfer of identity documents."[94] The 1998 addition of paragraph (a)(7) "expanded the definition of 'means of identification' to include such information as [Social Security Numbers] and other government identification numbers, dates of birth, and unique biometric data (e.g., fingerprints), as well as electronic access devices and routing codes used in the financial and telecommunications sectors."[95]

B. STATE IDENTITY THEFT LAWS

Forty-eight states currently have identity theft laws.[96] The first state to pass a law recognizing identity theft as an independent crime[97] was Arizona in 1996.[98] Most of the other states, except Colorado and Vermont,[99] have

---

[92] *Id.*

[93] *Id.*

[94] GAO, *supra* note 83, at 5.

[95] *Id.*

[96] *See* FED. TRADE COMM'N, IDENTITY THEFT STATE LAWS, *at* http://www.consumer.gov/idtheft/federallaws.html#statelaws (revised Dec. 20, 2002) (listing the state identity theft laws) [hereinafter FTC (STATE LAWS)]. Furthermore, the GAO survey states that in 1998 (at the time the federal law was passed) only a few states had specific laws dealing with the problem of identity theft. GAO, *supra* note 83, at 6. But currently, the FTC reports that forty-eight states have laws that address identity theft; only Colorado and Vermont have not yet passed an identity theft law. FTC (STATE LAWS), *supra*. However, while Colorado may not have a statute dealing with identity theft specifically, Colorado has a statute making criminal impersonation a felony. *See* COLO. REV. STAT. ANN. § 18-5-113 (West 2002). Furthermore, although Vermont has not yet passed an identity theft law, in 2003, the Vermont Legislature introduced a bill "propos[ing] to create the crime of identity theft." H.B. 200, 2003-2004 Leg. Sess. (Vt. 2003).

[97] That is not to say that before an identity theft law was passed that identity thieves could not be prosecuted. Identity thieves could be prosecuted under other criminal laws such as criminal misrepresentation or forgery laws. However, this was the first law to recognize identity theft as an independent crime.

[98] GAO, *supra* note 83, at 7; *see also* ARIZ. REV. STAT. ANN. § 13-2008 (West 2001 & West Supp. 2003). The GAO reports that Mississippi may have actually been the first state

followed Arizona and have enacted statutes dealing with identity theft to some extent, some before and others after ITADA was passed in 1998.[100]

Each state's identity theft statute is unique.[101] However, with respect to criminal record identity theft, the state identity theft laws can be grouped into three general categories. The first category includes states with very narrow identity theft statutes, focusing only on identity theft for financial purposes.[102] Some of these states even label the crime as "financial identity fraud."[103] A plain reading of these statutes seems to leave no room for prosecution of criminal record identity theft, thus leaving a victim of criminal record identity theft with no recourse under the state identity theft law.[104]

The second type of state identity theft statutes are a bit broader. These statutes include an open ended, catch-all phrase stating that identity theft is a crime for financial purposes and/or "for any unlawful activity."[105] These statutes may include criminal record identity theft as a crime.[106]

---

to pass a law dealing with identity theft when it passed a "false pretences" statute (MISS. CODE ANN. § 97-19-85 (2000)) even though it was not labeled an "identity theft" statute. GAO, *supra* note 83, at 7. This statute was first passed in 1993, but was later amended in 1998 to include additional identifiers and also changed the punishment from a misdemeanor to a felony. *Id.*

[99] *See* FTC (STATE LAWS), *supra* note 96.

[100] GAO, *supra* note 83, at 6.

[101] The purpose of this section is not to provide a comprehensive explanation of each state's identity theft law. Rather, this section will look at specific state laws as examples in order to illustrate different issues and problems that may arise in the context of criminal record identity theft.

[102] *See, e.g.*, IDAHO CODE § 18-3126 (Michie Supp. 2003) ("It is unlawful for any person to obtain . . . or attempt to obtain, credit, money, goods or services, in the name of the other person . . . ."); W. VA. CODE ANN. § 61-3-54 (Michie 2000) ("Any person who knowingly takes . . . identifying information of another person . . . with the intent to fraudulently represent that he or she is the other person for the purpose of making financial or credit transactions in the other person's name . . . ."). These statutes are representative, but by no means an exhaustive list, of such statutes.

[103] *See, e.g.*, ARK. CODE ANN. § 5-37-227 (Michie Supp. 2003) ("Financial Identity Fraud"); 720 ILL. COMP. STAT. ANN. 5/16G-1 (West 2003) ("Financial Identity Theft and Asset Forfeiture Law"). *But see* S.B. 242, 93rd Gen. Assem., Reg. Sess. (Ill. 2003), a bill that passed the Illinois State Senate on July 31, 2003 which amended the narrow Illinois identity theft law so that the law could encompass more than just financial identity theft. Specifically, the new law changed all references to "financial identity theft" to read "identity theft" and to add language to the statute that would criminalize the use of personal identification information for reasons other than financial purposes.

[104] *But see supra* note 97 and accompanying text (explaining that although a victim may have no recourse under the identity theft statute, the victim may be able to bring her claim, or the thief may be prosecuted, pursuant to another state law).

[105] *See, e.g.*, ARIZ. REV. STAT. § 13-2008 (A) (West Supp. 2003) (stating that identity theft is a crime if the thief "knowingly takes, uses, sells or transfers any personal identifying

Finally, a minority of state laws have provisions addressing criminal record identity theft directly.[107] These statutes explicitly criminalize the use of a victim's personal identification "to commit a crime"[108] or "to avoid identification, apprehension, or prosecution for a crime."[109]

Thus, prosecution for criminal record identity theft can certainly occur under statues in the third category, possibly under statutes in the second category, and very unlikely under statutes in the first category. Whether a criminal record identity thief is subject to prosecution under a specific criminal record provision or under a broad open ended provision could have significant consequences, especially when determining how to punish the identity thief.

1. Variation in Punishment

Because some criminal record identity thieves may be prosecuted under specific criminal record provisions in the statutes,[110] while others may be prosecuted under broad open ended provisions in the statutes,[111] the resulting punishment for a criminal record identity theft can vary widely from state to state. The variation in punishment can occur at two levels:

---

information of another person . . . *for any unlawful purpose* or to cause loss to a person whether or not the person actually suffers any economic loss as a result of the offense") (emphasis added); 18 PA. CONS. STAT. ANN. § 4120(a) (West Supp. 2003) ("A person commits the offense of identity theft of another person if he possesses or uses, through any means, identifying information of another person without the consent of that other person to further *any unlawful purpose*.") (emphasis added). While many states use the language "any unlawful activity," other states have similar provisions using different open ended language. *See, e.g.*, ME. REV. STAT. ANN. tit. 17-A, § 905-A(C) (West Supp. 2002) (stating that it is a crime if one "[p]resents or uses a form of legal identification that that person is not authorized to use"). Even in states where identity theft is a crime "for any unlawful activity," many statutes have provisions specifically excluding those under twenty-one who obtain false identification in order to purchase alcohol or for someone under eighteen who uses false identification to purchase tobacco. *See, e.g.*, ALA. CODE § 13A-8-192(d) (Supp. 2002) (stating that identity theft law is not applicable when identity is obtained to "misrepresent his age for the sole purpose of obtaining alcoholic beverages, tobacco, or another privilege denied to minors"); KY. REV. STAT. ANN. § 514.160(3) (Michie Supp. 2003) (stating that law does not apply if one "misrepresent[s] his or her age for the purpose of obtaining alcoholic beverages, tobacco, or another privilege denied to minors").

[106] The ITADA is similar to the state laws that contain open ended language making identity theft a crime for "any unlawful activity." *See* 18 U.S.C. § 1028(a)(7) (2000).

[107] *See supra* note 86 and accompanying text.

[108] CAL. PENAL CODE § 530.5 (c) (West. 1999 & West Supp. 2003).

[109] MD. CODE ANN., CRIMINAL LAW § 8-301(c)(1) (2002 & Supp. 2003).

[110] *See supra* notes 108-09 and accompanying text.

[111] *See supra* notes 105-06 and accompanying text.

criminal record versus financial identity theft within a single state and criminal record identity theft between different states.

a. Felony v. Misdemeanor

The penalty for identity theft varies among the states. Some states consider identity theft a felony, regardless of whether the crime was for financial or criminal record purposes.[112] But a few states consider identity theft of any form only a misdemeanor.[113]

However, several states differentiate financial and criminal record identity theft and vary the penalty accordingly.[114] This differentiation could have significant consequences for prosecuting criminal record identity thieves. For example, in North Carolina criminal record identity theft is a higher-graded felony, carrying a higher penalty than financial identity theft.[115] In contrast, Nevada considers criminal record identity theft a lower-graded felony than financial identity theft.[116] Moreover, a financial identity thief in Nevada can be further punished by a fine of up to $100,000,[117] but no additional fine or penalty may be imposed on a criminal record identity thief.[118] Thus, in Nevada a criminal record identity thief cannot be punished as harshly as a financial identity thief.[119]

---

[112] *See, e.g.*, OKLA. STAT. ANN. tit. 21, § 1533.1(D) (West Supp. 2002) ("Identity theft is a felony offense"); WIS. STAT. ANN. § 943.201 (2) (West Supp. 2003) ("Whoever . . . intentionally uses . . . or attempts to use any personal identifying information or personal identification document of an individual . . . is guilty of a Class H felony.").

[113] *See, e.g.*, N.M. STAT. ANN. § 30-16-24.1 (C) (Michie Supp. 2003) ("Whoever commits theft of identity is guilty of a misdemeanor."); S.D. CODIFIED LAWS § 22-30A-3.1 (2) (Michie Supp. 2003) ("Class 1 misdemeanor"); TENN. CODE ANN. § 39-16-301 (b) (2003) ("Class B misdemeanor").

[114] *See infra* notes 115-28 and accompanying text (providing examples of state laws that vary the penalty based on the violation).

[115] N.C. GEN. STAT. § 14-113.22 (2001) (classifying financial identity theft as a Class G felony and criminal record identity theft as a Class F felony); *see also* VA. CODE ANN. § 18.2-186.3(D) (Michie Supp. 2003) (stating that a violation is a Class 1 misdemeanor, but "[a]ny violation resulting in the arrest and detention of the person whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony").

[116] NEV. REV. STAT. ANN. 205.463 (Michie 2001) (classifying financial identity theft and identity theft for "any unlawful purpose" as a category B felony and criminal record identity theft as a category E felony).

[117] *Id.* 205.463 (1)(b).

[118] *See id.* 205.463 (2)(b) (stating that the crime is punishable as a category E felony, with no mention of an additional fine available).

[119] *See also* MD. CODE ANN., CRIMINAL LAW § 8-301(c)(1), (d) (2002 & Supp. 2003) (recognizing that "to avoid identification, apprehension or prosecution for a crime" is crime, but such a violation is only a misdemeanor whereas financial identity theft resulting in a loss

Another way in which the variation of the penalty may affect criminal record identity theft is when the penalty directly corresponds with the amount of resulting financial loss to the victim.[120] While such penalties may seem to imply that the state has a narrow financial identity theft law, leaving no room to prosecute for criminal record identity theft, identity theft resulting in "no financial loss"[121] or "no economic benefit"[122] is still a crime in some states. Therefore, statutes that vary the penalty based on the amount of financial loss are not necessarily limiting the crime only to financial identity theft, but the punishments for criminal record identity theft usually correspond with the lowest monetary threshold for punishing financial identity theft.[123] In Alabama, for instance, identity theft resulting in *no financial loss* or a loss of less than $250 is a misdemeanor.[124] However, identity theft involving financial loss of more than $250 is a felony.[125] The plain reading of the Alabama statute, therefore, classifies criminal record identity theft, which results in no financial loss, but has other devastating effects,[126] only as a misdemeanor. In contrast to Alabama, however, Virginia explicitly makes criminal record identity theft a felony, even though identity theft resulting in a financial loss of less than $200 is only a misdemeanor.[127]

Whether or not laws similar to Alabama intend to treat criminal record identity theft as the lowest possible offense or are doing so unintentionally by default is unclear. On the one hand, the Alabama law does not explicitly limit identity theft to financial identity theft.[128] On the other hand, a criminal record identity thief will, at best, be punished with the most lenient

---

of $500 or greater is a felony).

[120] *See, e.g.*, ALA. CODE § 13A-8-192(c) (Supp. 2002); IOWA CODE § 715A.8(3) (2003); MD. CODE ANN., CRIMINAL LAW § 8-301(d); MINN. STAT. ANN. § 609.527(3) (West 2003); MONT. CODE ANN. § 45-6-332(2) (2001); NEB. REV. STAT. § 28-608(2) (2002); OHIO REV. CODE ANN. § 2913.49(I) (West Supp. 2003); 18 PA. CONS. STAT. ANN. § 4120(c) (West Supp. 2003); WYO. STAT. ANN. § 6-3-901(c)(i) (Michie 2003).

[121] *See, e.g.*, ALA. CODE § 13A-8-192(c).

[122] *See, e.g.*, MONT. CODE ANN. § 45-6-332(2)(a); WYO. STAT. ANN. § 6-3-901(c)(i).

[123] *See, e.g.*, ALA. CODE § 13A-8-192.

[124] *Id.* § 13A-8-192(c) (stating that no financial loss or loss under $250 is a Class A misdemeanor, and $250 or more is a Class C felony).

[125] *Id.* § 13-A-8-192(b) (stating that $250 or more is a Class C felony).

[126] *See supra* notes 73-79 and accompanying text.

[127] VA. CODE ANN. § 18.2-186.3(D) (Michie Supp. 2003) (stating that a violation is a Class 1 misdemeanor, but any violation resulting in a loss greater than $200 or "[a]ny violation resulting in the arrest and detention of the person whose identification documents or identifying information were used to avoid summons, arrest, prosecution, or to impede a criminal investigation shall be punishable as a Class 6 felony").

[128] *See supra* notes 121-22 and accompanying text.

class of financial identity thieves.[129] Thus, states that make the economic loss the threshold for severity of liability may be allowing a criminal record identity thief to get away with the lowest possible punishment or no punishment at all.

b. Repeat Offenders

Another way in which the state identity theft laws differ with respect to criminal record identity theft is how repeat offenders are punished. Some identity theft laws vary the penalty based on whether or not the crime was the thief's first offense.[130] For example, the New York identity theft laws classify three types of identity theft: identity theft in the third degree,[131] second degree,[132] and first degree.[133] The laws provide that one who commits identity theft in the *third* degree, but within the last five years was convicted of identity theft in the first, second, or third degree, the offense is increased to identity theft in the *second* degree.[134] Similarly, one who commits identity theft in the *second* degree, but within the last five years was convicted of identity theft in the first, second, or third degree, the offense is increased to identity theft in the *first* degree.[135] Because New York recognizes criminal record identity theft as a crime at each level, the harsher punishment imposed on a repeat offender will likely work for punishing a criminal record identity thief as well.[136]

However, Nebraska does not seem to treat a repeat criminal record identity thief as harshly as most repeat financial identity thieves.[137] In Nebraska, one who commits identity theft when "no[thing] . . . of value was gained," commits a class II misdemeanor.[138] Although a second conviction

---

[129] *See supra* notes 124-26 and accompanying text.

[130] *See, e.g.*, N.Y. PENAL LAW §§ 190.79-.80 (Consol. Supp. 2003) (stating that if someone commits identity theft in the third degree, but within the last five years the thief committed identity theft in the first, second, or third degree, the offense is increased to identity theft in the second degree. Similarly, if one commits identity theft in the second degree, but within the last five years the thief committed identity theft in the first, second, or third degree, the offense is increased to identity theft in the first degree.); *see also* VA. CODE ANN. § 18.2-186.3(D) (stating that a violation is a Class 1 misdemeanor, but "[a]ny second or subsequent conviction shall be punishable as a Class 6 felony").

[131] N.Y. PENAL LAW § 190.78.

[132] *Id.* § 190.79.

[133] *Id.* § 190.80.

[134] *Id.* § 190.79 (4).

[135] *Id.* § 190.80 (4).

[136] *See, e.g.*, *id.* § 190.78(2).

[137] *See* NEB. REV. STAT. § 28-608(2)(d) (Supp. 2002).

[138] *Id.*

under this section is punishable as a higher-graded class I misdemeanor,[139] repeat financial identity theft involving $200 or more is punished at least as a class IV felony, not a class I misdemeanor.[140] Thus, in Nebraska, a second time criminal record identity thief is subject to a more lenient punishment than almost all repeat financial identity thieves.[141]

Harsher punishments for repeat offenders are important for another reason in the context of criminal record identity theft. Some identity thieves obtain identities of multiple victims and use one victim's identity for financial purposes and another victim's identity to avoid arrest from the first identity theft incident.[142] For example, in a recent Chicago case, an identity thief from Indiana attempted to withdraw $200,000 using the identity of a suburban Chicago victim.[143] The suspicious bank teller phoned the Chicago man and discovered that he was at home, and the one attempting to withdraw money in his name was an identity thief.[144] When the police subsequently arrived, the identity thief provided the name and identification of an Oregon man, a second identity theft victim, to prevent the arrest and attempted crime from appearing on his own criminal record.[145] In this case, the identity thief was attempting to commit both financial and criminal record identity theft arising from a single incident. In other cases, however, an identity thief may use the identification of a different victim for each offense to avoid the harsher punishments imposed on repeat offenders.[146]

2. State Law Provisions Intended to Assist Victims of Criminal Record Identity Theft

Because the victim usually bears the burden of having her erroneous criminal record cleared, some state statutes have provisions to help alleviate the victim's burden by permitting or ordering the court to correct the

---

[139] *Id.*

[140] *Id.* § 28-608(2)(c).

[141] *See id.* § 28-608(2). *But see id.* § 28-608(2)(d) (stating that a repeat financial identity theft involving $200 or less is subject to the same punishments as a repeat identity theft where "no[thing] . . . of value was gained" and a third offense in this category is punished as a class IV felony). Thus, in Nebraska, a second time criminal record identity thief receives a lower punishment than all repeat financial identity thieves where the thief gained $200 or more.

[142] Telephone Interview with Sophia Lopez, Supervisor of Consumer Fraud Division, Cook County State's Attorney's Office (Mar. 12, 2003) (notes on file with author).

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.*

victim's criminal record.[147] In Georgia, for example, a "court may issue any order necessary to correct a public record that contains false information resulting from [an erroneous] conviction."[148] Similarly, in North Carolina, a victim of criminal record identity theft may have the court "reflect that [the victim] did not commit the crime."[149] Utah and Wyoming have similar provisions as well.[150]

California's identity theft laws[151] address criminal record identity theft, and many of the problems presented to the victims, in more detail than most other states.[152] In addition to overtly recognizing the crime of criminal record identity theft,[153] California requires the state's Department of Justice to establish a database to assist identity theft victims.[154] The law also allows a victim to initiate a law enforcement investigation,[155] and assists the victim in having her record's cleared by allowing the victim to "petition a court . . . for an expedited judicial determination of his or her factual innocence."[156] Thus, beyond recognizing criminal record identity theft as an independent crime, state legislatures can follow California's lead and build into their identity theft statutes methods by which the unique problems associated with the crime may be addressed to alleviate the burden that usually falls on the victim.[157]

---

[147] *See, e.g.*, CAL. PENAL CODE § 530.6 (West Supp. 2003); GA. CODE ANN. § 16-9-126(d) (Supp. 2002); N.C. GEN STAT. § 14-113.22(c) (2001); UTAH CODE ANN. § 76-6-1104 (Supp. 2003); WASH. REV. CODE ANN. § 9.35.020(6) (West 2003); WYO. STAT. ANN. § 6-3-901(e) (Michie 2003).

[148] GA. CODE ANN. § 16-9-126(d). The Georgia law is a good example of a state law that does not expressly recognize criminal record identity theft, but has open ended language that would allow for prosecution of criminal record identity theft. *See id.* § 16-9-121(1)-(2). Notwithstanding the lack of express language regarding criminal record identity theft, the law does provide the victim with an avenue to alleviate her burden of clearing an erroneous record. *Id.* § 16-9-126(d).

[149] N.C. GEN. STAT. § 14-113.22(c).

[150] UTAH CODE ANN. § 76-6-1104; WYO. STAT. ANN. § 6-3-901(e).

[151] CAL. PENAL. CODE §§ 530.5-.8 (West Supp. 2003).

[152] For a more detailed explanation of the provisions of the California law, *see infra* notes 231-35 and accompanying text.

[153] CAL. PENAL CODE § 530.5(c).

[154] *Id.* § 530.7(c). Once a victim reports to the Department of Justice, the Department is required to "verify the identity of the victim against any driver's license or other identification record maintained by the Department of Motor Vehicles." *Id.* § 530.7(b).

[155] *Id.* § 530.6(a).

[156] *Id.* § 530.6(b). If the victim is found factually innocent, "the court shall issue an order certifying this determination." *Id.*

[157] *See supra* notes 73-79 and accompanying text.

3. State Law Provisions Addressing the Appropriate Venue for Prosecution

One problem that prosecutors often face when prosecuting identity theft[158] is finding the appropriate venue in which to prosecute.[159] For example, an identity thief living in state *A* may obtain the personal information of a victim domiciled in state *B*, and use that information to carry out her crime in state *C* or *D*.[160] Moreover, an identity thief who carries out her crime, even in part, over the Internet can further complicate the venue determination.[161] Recognizing this potential dilemma, some states allow prosecution to take place "in any locality where the person whose identifying information was appropriated resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in such locality."[162]

Even if an identity theft statute relaxes the venue requirement, the "realistic practicalities" of prosecuting identity thieves in one of those venues may be problematic[163] because an identity thief may be nowhere near any of those venues authorized by the state's statute. If the alleged identity thief is reluctant to cooperate with the prosecutor and is unwilling to voluntarily appear at any hearings, the defendant would have to be

---

[158] Finding the appropriate venue is relevant to all forms of identity theft. However, the ramifications of finding the appropriate venue are just as relevant to criminal record identity theft as they are to other forms of identity theft. Similarly, the statute of limitations issue, which will be discussed below, is relevant to criminal record identity theft as well as other forms of identity theft. *See infra* notes 171-89 and accompanying text.

[159] L.A. Lorek, *Stolen Identity; Law Enforcement Can't Keep Up with Electronic-Age Crime*, SAN ANTONIO EXPRESS NEWS, Sept. 12, 2002, at 1E. Similarly, at the state level, instead of states *A*, *B*, or *C* as explained above, the problem of where to prosecute could be among counties *A*, *B*, or *C*. *See id.*

[160] *Id.*

[161] *See supra* notes 34-38 and accompanying text.

[162] VA. CODE ANN. § 18.2-186.3(D) (Michie Supp. 2003); *see also* FLA. STAT. ANN. § 817.568(9) (West Supp. 2003) ("venue . . . may be commenced and maintained in any county in which an element of the offense occurred, including the county where the victim generally resides."); KY. REV. STAT. ANN. § 514.160(5) (Michie 2002) ("venue . . . may be in either the county where the offense was committed or the county where the other person resides."); N.M. STAT. ANN. § 30-16-24.1(E) (Michie Supp. 2003); N.C. GEN. STAT. § 14-113.21 (2001); 18 PA. CONS. STAT. ANN. § 4120(e.1) (West Supp. 2003); UTAH CODE ANN. § 76-6-1103(1) (Supp. 2003); WASH. REV. CODE ANN. § 9.35.020(4) (West 2003) ("In a proceeding under this section, the crime will be considered to have been committed in any locality where the person whose means of identification or financial information was appropriated resides, or in which any part of the offense took place . . . .").

[163] Telephone Interview with Sophia Lopez, *supra* note 12 (explaining that many states even have general venue statutes which permit prosecution in any state where any part of the crime took place, but the true problem is the difficulty of extraditing the defendant to the place of prosecution).

extradited.[164] Extradition is an expensive proposition requiring detectives and other techniques and resources to find and bring the defendant to the appropriate location.[165] Such expensive undertakings by state prosecutors are usually reserved for high profile felonies such as murder.[166] Thus, even if venue is appropriate there may be realistic practicalities that prevent prosecution of identity thieves.

C. ISSUES NOT ADDRESSED BY STATE IDENTITY THEFT LAWS

Although a minority of state identity theft laws expressly address criminal record identity theft, almost all state identity theft laws fail to address two issues. First, state laws fail to recognize the issue associated with the statute of limitations in the identity theft context.[167] Similar to the venue difficulty, the statute of limitations issue is relevant to all forms of identity theft, not only criminal record identity theft.[168] Second, even the states that address criminal record identity theft do not address "reverse criminal record identity theft,"[169] a specific form of criminal record identity theft.[170]

1. Statute of Limitations

Because an identity thief may be using the victim's personal information for an extended period of time before the victim becomes aware that she is being victimized, when the statute of limitations begins to run is unclear.[171] In other words, does the statute of limitations begin to run from the time that the identity thief obtains the victim's personal information, from the time the identity thief actually begins using the victim's information, from the time that the victim learns that the thief is

---

[164] *Id.*

[165] *Id.*

[166] *Id.* That is not to say that an identity theft crime cannot rise to a level where extradition would be appropriate. However, most identity theft crimes will not rise to this level and thereby not justify the costs associated with extradition.

[167] *But see* FLA. STAT. ANN. § 817.568(10) (West Supp. 2003) (stating there is a three year statute of limitations beginning from the time the offense occurred). However, a claim may still be brought within one year from the time the victim learned of the offense as long as it is still within five years from when the offense occurred. *Id.*

[168] *See supra* note 158 and accompanying text.

[169] *See supra* notes 63-66 and accompanying text.

[170] *But see* MICH. COMP. LAWS ANN. § 750.285(1)(c) (West Supp. 2003) (stating that it is a crime to use a person's personal identification information "to obtain employment").

[171] *See supra* note 53 and accompanying text (reporting that it takes the average victim 12.3 months before learning that she has been victimized).

using her personal information unlawfully, or at some other point in the process?

a. Supreme Court: *TRW Inc. v. Andrews*

Although most state identity theft laws do not address the statute of limitations issue directly,[172] in 2001 the Supreme Court addressed the issue in *TRW Inc. v. Andrews*,[173] an identity theft case brought under The Fair Credit Reporting Act ("FCRA").[174] In the first identity theft case heard by the Supreme Court,[175] the Court held that the statute of limitations begins to run when the identity thief begins using the victim's information, not from the time that the victim learned of the identity theft.[176] Although the Court's holding has justifiably been criticized for refusing to apply the general discovery rule for the time when the statute of limitations begins to run,[177] the ramifications of *TRW* are unclear. On the one hand, since FCRA specifically provides that a claim may only be brought "within two years from the date on which the liability arises,"[178] *TRW*'s holding may be limited to identity theft claims brought under FRCA. But if the claim was brought pursuant to some other statute, then perhaps the Ninth Circuit's application of the "general federal rule . . . that a federal statute of limitations begins to run when a party knows or has reason to know that she

---

[172] *But see supra* note 167 and accompanying text.

[173] 534 U.S. 19 (2001).

[174] *Id.* (addressing the statute of limitations issue arising out of a claim brought by an identity theft victim against a credit reporting agency under FCRA, codified as 15 U.S.C. § 1681 (1994), for unauthorized disclosure of the victim's credit information).

[175] Erin M. Shoudt, Comment, *Identity Theft: Victims "Cry Out" for Reform*, 52 AM. U. L. REV. 339, 340 (2002) (noting that it was the first identity theft case heard by the Supreme Court).

[176] The case was brought by an identity theft victim pursuant to FCRA against TRW, a credit reporting agency. The claim was brought within two years from the time the victim learned that she had become a victim, but not within two years from when the alleged disclosure took place. The victim claimed that the credit agency violated FCRA by releasing the victim's credit information without her consent. However, § 1681p of FCRA states that an action may be brought "within two years from the date on which the liability arises, except that where a defendant has materially and willfully misrepresented any information required . . . to be disclosed . . . ." 15 U.S.C. § 1681p. In reversing the Ninth Circuit's application of the "general federal rule . . . that a federal statute of limitations begins to run when a party knows or has reason to know that she was injured" *TRW*, 534 U.S. at 26 (citing Andrews v. TRW Inc., 225 F.3d 1063, 1066 (9th Cir. 2000)), the Court held that since FCRA specifically creates a two year statute of limitations with a specified exception, the general federal discovery rule is inapplicable to FRCA.

[177] *See* Shoudt, *supra* note 175, at 356-62.

[178] 15 U.S.C. § 1681p.

was injured"[179] would have been correct. Moreover, *TRW* was a civil case under FCRA whereas the state identity theft laws are criminal laws.[180] On the other hand, a broader reading of the holding could suggest that in identity theft cases in general, the statute of limitations begins to run from the time the identity thief commits the crime, not when the victim learns of the crime.[181]

b. State Action Necessary

With the uncertainty of the application of *TRW*'s holding to state-law identity theft claims, and the risk that victims will be unable to seek recourse due to a potential lapse of the statute of limitations, a comprehensive identity theft law would include a provision addressing the statute of limitations directly. Because identity theft laws are relatively new,[182] 12.3 months pass before the average victim learns that she has been victimized,[183] and the statute of limitations would have to expire in order for a victim to have standing to challenge the relevant statute of limitations, the statute of limitations issue is likely to arise in the near future.[184]

The Florida identity theft law is unique because it contains a provision addressing the statute of limitations problem.[185] The Florida law provides a three year statute of limitations commencing from the time the offense occurred.[186] However, a victim may still bring a claim within one year from the time the victim learned of the offense as long as the claim is brought within five years from when the offense occurred.[187] Although the Florida law does not provide the victim with the ultimate protection of preventing the statute of limitations from running until the victim is aware that she has

---

[179] *TRW*, 534 U.S. at 26 (citing *Andrews*, 225 F.3d at 1066).

[180] While all states that have identity theft laws make identity theft a crime to some degree, some states have additional laws that allow the victim to pursue a civil action against the thief. *Compare* CONN. GEN. STAT. § 53a-129a (2001) (Class D Felony) *with* CONN. GEN. STAT. § 52-571h (Supp. 2003) (civil action for damages); *compare* IOWA CODE § 715A.8 (2003) (criminal) *with* IOWA CODE § 714.16B (civil cause of action); *compare* TENN. CODE ANN. § 39-14-150 (2002) (criminal) *with* TENN. CODE ANN. § 47-18-2105 (2001) (civil).

[181] *See* Shoudt, *supra* note 175, at 356 (criticizing the holding in *TRW* and suggesting that the FCRA should be amended so that the statute of limitations begins to run from the time the victim discovers the offense).

[182] *See supra* note 96 and accompanying text.

[183] *See supra* note 53 and accompanying text.

[184] Given these factors it would seem that the issue will arise more frequently in the future, even if the issue has not yet arisen.

[185] FLA. STAT. ANN. § 817.568(10) (West Supp. 2003); *see supra* note 167 and accompanying text.

[186] *Id.*

[187] *Id.*

been victimized,[188] a victim who learns about the crime within five years may still seek recourse under the Florida law. However, a victim who remains unaware that she has been victimized for five years or longer has no recourse even under the Florida law.[189]

2. Reverse Criminal Record Identity Theft

The states recognizing criminal record identity theft as a crime[190] generally do not address reverse criminal record identity theft.[191] As explained above, this form of identity theft often arises when one is unable to obtain a job because a background check of the applicant reveals a criminal record.[192] By assuming the identity of a victim with a clean criminal record, the job applicant may avoid detection that a background check would otherwise reveal.[193]

States that specifically criminalize criminal record identity theft generally refer to the crime as using the victim's identity to avoid arrest or prosecution.[194] Under these provisions, reverse criminal record identity

---

[188] *See* Shoudt, *supra* note 175, at 389 (suggesting that amending the FCRA to apply the injury discovery rule would "have the most significant impact on victims of identity theft").

[189] While it may seem unlikely for five years to pass before a victim learns that she has been victimized, the FTC reports that sixteen percent of victims did not learn that their personal identification was being misused for more than two years from the time of the initial misuse. FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 6. This is in contrast to the sixty-nine percent of victims who reported discovering that they were victims within six months of the first occurrence, and the forty-four percent who even discovered within the first month. *Id.* However, the average time, 12.3 months, that it takes for a victim to learn that she has become a victim is "about twice as long as the majorities' experience . . . due to the skewing effect of the smaller number of victims who did not discover the identity theft for two years or longer." *Id.* Thus, the statute of limitations provision in the Florida law would seem to cover most, but not all, identity theft victims.

[190] *See supra* note 86 and accompanying text.

[191] *See supra* notes 63-66 and accompanying text (discussing reverse criminal record identity theft).

[192] The FTC reports that in 2001, nine percent of identity theft victims claimed that their personal information was used by the thief to secure employment. FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 3 (referring to this as "employment fraud").

[193] *See, e.g.*, Solida, *supra* note 62, at 1A (stating that convicted felon passed a background check and was hired for a job by providing the date of birth and Social Security Number of someone with the applicant's same name to avoid having his criminal convictions hurt his chances for the job).

[194] *See, e.g.*, NEV. REV. STAT. ANN. § 205.463(2)(b) (Michie 2001) (stating that it is a crime to use someone's personal information to "avoid or delay being prosecuted for an unlawful act"); VA. CODE ANN. § 18.2-186.3(B) (Michie Supp. 2003) (stating that it is violation of the law to use the personal information of someone else to "avoid summons, arrest, prosecution, or to impede a criminal investigation"). These statutes are examples illustrating that the common statute criminalizing criminal record identity theft addresses the

theft would not seem to constitute a crime. However, the states that include provisions that criminalize identity theft for "any unlawful activity"[195] could potentially include reverse criminal record identity theft as a violation of the law.[196] After all, misrepresenting one's self as someone else to obtain a job may be deemed an "unlawful activity."[197] Thus, statutes that only criminalize traditional criminal record identity theft may be too narrow to include reverse criminal record identity theft as a crime as well.[198]

Although most states fail to address reverse criminal record identity theft, Michigan expressly prohibits the use of personal identification "to obtain employment."[199] However, with the exception of Michigan, most statutes do not seem to address reverse criminal record identity theft at all; not as an independent crime, nor as a subset of another form of identity theft.[200]

---

situation where the identity thief uses the victim's personal information to avoid prosecution or arrest. Under statutes like these, there does not seem to be any room to prosecute for reverse criminal record identity theft. For a list of other similar statutes, see *supra* note 86 and accompanying text.

[195] *See supra* note 105 and accompanying text.

[196] I consider reverse criminal record identity theft a subset of criminal record identity theft. However, an argument could be made that if the identity thief is using the victim's personal information to get a job, and ultimately a salary, then this form of identity theft is more akin to financial identity theft than criminal record identity theft. But the wrongdoing of the identity thief is not stealing the victim's money; rather, the thief is using the victim's clean criminal record to obtain the job. Ultimately, the identity thief is the one working for and earning her wages, albeit under the victim's identity. The wrong only occurs when the thief uses the victim's clean record to secure a job and therefore constitutes a form of criminal record identity theft. Furthermore, while reverse criminal record identity theft is a subset of classic criminal record identity theft, there does not seem to be a parallel form of reverse financial identity theft. At first glance, it may seem that an identity thief who files a bankruptcy petition using the victim's name to obtain a discharge for the debts the thief incurred in the victim's name, would be parallel to reverse criminal record identity theft; however, unlike reverse criminal record identity theft, which does not cause any actual harm to the victim beyond her personal information being used by some stranger, when the thief files for bankruptcy in the victim's name, the victim is adversely affected. *See supra* note 49 and accompanying text.

[197] If a state has an independent crime of misrepresentation then the identity thief may be liable under the "any unlawful activity" clause of the identity theft statute as well. *See, e.g.*, COLO. REV. STAT. ANN. § 18-5-113 (West 2002) (recognizing "Criminal impersonation" as an individual crime). But if no such statute exists and the violation is not included in the identity theft statute, then it may not be so obvious that the identity thief did anything "unlawful." He may have lied and been dishonest, but perhaps there is no recourse for such actions.

[198] For examples of narrow criminal record identity theft statutes, see *supra* note 86 and accompanying text.

[199] MICH. COMP. LAWS ANN. § 750.285(1)(c) (West Supp. 2003).

[200] *But see, e.g.*, TENN. CODE ANN. § 39-14-150(b)(1) (2002) (including "employer or

While states are beginning to recognize that identity theft does not only occur for financial purposes, reverse criminal record identity theft illustrates the need for legislatures to constantly be aware of new ways in which identity thieves may act.[201] Reverse criminal record identity theft demonstrates that laws only addressing classic financial or criminal record identity theft directly, while necessary, are insufficient to address new forms of identity theft that may arise. Thus, in addition to provisions expressly addressing financial and criminal record identity theft, open-ended language is necessary to enable prosecution of reverse criminal record identity theft or any new forms of identity theft that may arise.[202]

D. A MODEL IDENTITY THEFT LAW

The only apparent uniformity among the state identity theft laws is that all the laws address identity theft in some form. However, the laws collectively suggest the necessary provisions that a comprehensive identity theft law would contain. A thorough law would expressly address financial, criminal record,[203] and reverse criminal record identity theft.[204] The law would also contain broad, open-ended language leaving room for prosecution of new forms of identity theft that may arise.[205]

With respect to punishment, most forms of identity theft would be felonies.[206] However, states should have a monetary threshold in order for the crime of financial identity theft to rise from a misdemeanor to a

---

taxpayer identification number" as personal information); OR. REV. STAT. § 165.800(4)(b)(E) (2001) ("employment status, employer or place of employment"); N.D. CENT. CODE § 12.1-23-11(1)(f) (Supp. 2003) ("employer or place of employment"). However, it is unclear whether reverse criminal record identity theft would fall under these provisions.

[201] *Cf.* Peter Huck, *Identity Thieves Leave the Unwary Paying the Bills,* THE AGE (MELBOURNE), Dec. 31, 2002, at 9 (stating that identity theft can be used by terrorists to launder money or create false names to obtain jobs).

[202] As mentioned earlier, many state identity theft statutes criminalize identity theft for "any unlawful activity." *See supra* note 105 and accompanying text. Under those laws, the activity must be "unlawful" in order to be able to prosecute under this clause of the statute. *See supra* note 197 and accompanying text. However, the Ohio identity theft statute has unique open ended language that seems to criminalize, in a generic way, many activities that would not otherwise be included in the statute or included in the language of "any unlawful activity." OHIO REV. CODE ANN. § 2913.49(B)(1) (West Supp. 2003) (stating that it is a crime to "[h]old the person out to be the other person").

[203] For examples of laws that mention both financial and criminal record identity theft, see *supra* note 86 and accompanying text.

[204] *See, e.g.*, MICH. COMP. LAWS ANN. § 750.285(1)(c) (West Supp. 2003).

[205] *See supra* note 202 and accompanying text.

[206] *See supra* note 112 and accompanying text.

felony.[207] Meaning, financial identity theft involving less than $250, for example, would be a misdemeanor and anything above $250 would be a felony. But a law with a monetary threshold distinguishing between a felony and a misdemeanor would expressly recognize criminal record identity theft as a felony. This is necessary so that criminal record identity theft may be punishable as a felony and not only as a misdemeanor by default.[208] But even if financial and criminal record identity theft are clearly defined crimes, perhaps criminal record identity theft should carry a more severe penalty than a corresponding financial identity theft crime[209] due to the potentially devastating consequences of criminal record identity theft.[210]

Furthermore, all repeat offenders would be punished more severely than first time offenders, regardless of the form of identity theft.[211] Additionally, the law would contain provisions relaxing the venue restriction[212] and extending the statute of limitations to at least give every victim a chance to seek recourse under the law.[213] Finally, the law would include provisions to assist victims in clearing erroneous records[214] or set up a database similar to the one in California.[215]

IV. TWO WAYS CRIMINAL RECORD IDENTITY THEFT MAY BE CURTAILED

The recent rise in identity theft has caused the FTC, as well as others, to suggest ways to avoid becoming an identity theft victim.[216] Many scholars have argued that since preventing identity theft is difficult, individuals should take proactive measures to avoid being victimized.[217] In

---

[207] Telephone Interview with Sophia Lopez, *supra* note 12 (explaining that in a recent Chicago case, an identity thief attempted to use the victim's identity to order a twelve dollar pizza). Such a minor infraction should arguably only be a misdemeanor and not a felony. *Id.*

[208] *See supra* notes 120-29 and accompanying text.

[209] *See supra* notes 115-29 and accompanying text.

[210] *See supra* notes 73-79 and accompanying text.

[211] *See supra* notes 130-36 and accompanying text.

[212] *See supra* notes 158-62 and accompanying text. *But see supra* notes 163-66 (explaining that even if the venue requirement is relaxed or venue in a particular location is appropriate, there are realistic practicality difficulties that may prevent prosecution of some identity thieves).

[213] *See supra* notes 182-89 and accompanying text.

[214] *See supra* notes 147-50 and accompanying text.

[215] *See supra* notes 151-57 and accompanying text.

[216] *See, e.g.*, IDENTITY THEFT CLEARINGHOUSE, FED. TRADE COMM'N, PROTECTING AGAINST IDENTITY THEFT, *at* http://www.consumer.gov/idtheft/idtheftttesting/protect againstidt.html#5 (last visited Aug. 29, 2003); *see also* Hoar, *supra* note 24, at 1438-43.

[217] *See, e.g.*, Hoar, *supra* note 24, at 1438 ("While it is extremely difficult to prevent

general, these suggestions focus on what individuals can do to avoid becoming identity theft victims, including not carrying around one's Social Security Number in a wallet, securing home mail boxes, shredding all personal documents (including bank and credit card statements and all other documents containing personal identification information), and periodically checking credit reports.[218]

These suggestions generally focus on what individuals can do to protect themselves from becoming victims of identity theft. While individuals should take precautions to prevent identity thieves from obtaining their personal information, these suggestions do not help to prevent "inside jobs,"[219] or those identity thieves who assume the identity of family members or persons the identity thief knows.[220] Moreover, once someone has become a victim of identity theft, the suggestions of how to avoid becoming a victim are no longer helpful to prevent the identity thief from using the victim's identity for multiple purposes. Thus, the standard suggestions of how individuals may avoid becoming victims of identity theft are inadequate to solve the identity theft problem.

While there is no fool-proof way to avoid identity theft completely, increased interaction at the institutional level (in addition to preventative measures by individuals) seems necessary to prevent and control identity theft. This section will provide two methods of institutional action and intervention by which identity theft may be controlled and prevented: linking the intermediary parties between the identity thief and the victim and the increased use of biometric data.

---

identity theft, the best approach is to be proactive and take steps to avoid becoming a victim.").

[218] *Id.* at 1439-43.

[219] Identity thieves may obtain a victim's personal information from a company insider who has access to all of the victim's personal information. *See supra* notes 41-44 and accompanying text.

[220] The FTC reported that in 2001, thirteen percent of identity theft victims who contacted the FTC claimed "that they personally knew the person who had stolen and misused their identity." FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 8. Victims may "include family members (6%), friends, neighbors (2%) and persons known to the victim in a similar capacity (3%), roommates (1%), and personal associates from the victim's workplace (1%)." *Id.*; *see also* Lee v. Superior Court, 989 P.2d 1277 (Cal. 2000) (regarding a criminal record identity thief who assumed the identity of his deceased brother). Thus, taking precautionary measures, while important, will by no means eradicate identity theft completely.

A. THE NEED TO LINK THE INTERMEDIARY PARTIES BETWEEN THE IDENTITY THIEF AND VICTIM

The FTC reports that many identity thieves use the victim's information for multiple forms of identity theft.[221] Therefore, as any single type of identity theft increases, the risk of other forms of identity theft simultaneously increases.[222] Moreover, because the average identity theft victim remains unaware that she has been victimized for over a year,[223] even with well drafted identity theft laws[224] and detailed procedures for the victim to clear her name and record (credit or criminal), the victim must become aware that she is being victimized more quickly.

One possible method of achieving this early awareness is through increased and faster intervention by the intermediary parties between the victim and the thief. These parties include financial and credit institutions, law enforcement agencies, criminal record divisions of court houses, departments of motor vehicle, utility and telecommunication companies, and all other intermediary parties[225] that may be affected by potential identity thieves.[226] Not only would the link help prevent identity thieves from moving from one form of identity theft to another,[227] but it could

---

[221] FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 2 n.1.

[222] This is one of the reasons why it is important to look at criminal record identity theft in the context of other forms of identity theft. If identity theft is the fastest growing crime in America, the most common form of identity theft is for financial purposes, and many identity thieves use the victims' personal information for multiple forms of identity theft, then each form of identity theft has a direct impact on other forms of identity theft.

[223] *See supra* note 53 and accompanying text.

[224] For a detailed discussion of the necessary provisions for an effective state identity theft law, see *supra* Part III.

[225] See *supra* notes 45-67 and accompanying text for a discussion of all of the ways in which identity thieves use the victims' personal information and which agencies are potentially at risk for identity thieves.

[226] Because the vast majority of identity theft cases are financially motivated, the link between the intermediary parties can have an especially strong impact on criminal record identity theft. That is to say, the link between the intermediary parties may prevent or catch an identity thief who has already committed the crime for financial purposes from committing criminal record identity theft, as will be explained below.

[227] For example, assume that the identity thief obtains a victim's personal information and obtains a credit card and incurs substantial debt in the victim's name. Assume further that the victim becomes aware of this and notifies the credit card company and the credit reporting agency, and the victim's accounts are placed on fraud alert. If the police and department of motor vehicle are notified immediately, then if the identity thief attempts to continue using the victim's information the thief could be stopped, and more importantly, caught. If the police are notified, then when a driver is pulled over the police will pull up the driver's license number and see that there is a problem with this person's information. Although the police may not know immediately whether the one pulled over is the victim or the thief, it will cause the police to address the situation more carefully.

provide the victim with an opportunity to shift part of the burden that usually falls on her[228] to intermediary parties to address for her.[229] Thus, when an intermediary party becomes aware that someone has become an identity theft victim, that party should be required to notify the victim and ask the victim if she would like the incident reported to other intermediary parties.[230] If, however, the victim is concerned that contacting the other

---

[228] *See supra* notes 74-79 and accompanying text.

[229] It will only provide an *opportunity* because the victim will still have to decide if she wants the other intermediary parties to be notified. Privacy concerns still may prevent the intermediary parties from contacting each other without prior consent from the victim.

[230] There seem to be two ways in which such a link can be accomplished to limit the incidences of identity theft without compromising the victim's privacy rights, as suggested by FCRA. First, FCRA states a limited number of circumstances under which a consumer reporting agency may furnish a consumer credit report. 15 U.S.C. § 1681b (1994). These circumstances include "the order of a court having jurisdiction to issue such an order, or a subpoena issued in connection with proceedings before a Federal grand jury," and "[i]n accordance with the written instructions of the consumer to whom it relates." *Id.* § 1681b(1)-(2). Thus, the easiest way for the credit agencies to release the victim's information without raising any privacy issues would be the second method, the victim authorizing such disclosure. So for example, when a credit agency becomes aware of suspicious activity on the victim's credit report, the victim should be notified by the credit agency. This is possible because consumers are frequently notified when their credit card has unauthorized charges, and when a credit file is put on fraud alert. *See, e.g., U.S. Offers Reward in Theft of Military Data*, ST. LOUIS POST-DISPATCH, Jan. 1, 2003, at A11 (stating that when consumer files have fraud alerts on them, credit agencies are required to notify clients when credit applications are made in their name). Thus, when the victim is notified of these occurrences, the representative from the credit agency should inform the victim that perhaps she has been a victim of identity theft and that the identity thief may use or already be using the victim's information for other purposes, including criminal activity. At this point the victim would be able to make an informed decision whether or not she would like her information disclosed to other parties that may be able to stop the identity thief in her tracks. If the victim consents to such disclosure and puts the consent in writing, then the second method authorized by the FCRA would be satisfied. *See* 15 U.S.C. § 1681b(2). Similarly, if the victim does not consent to the disclosure, then the intermediary party has made the necessary effort to assist the victim, and by refusing to allow the disclosure, the victim assumes the risk that she will be victimized in other ways and will have the burden of dealing with the problem herself. If the intermediary party at least makes an effort to assist the victim, the victim then must perform a cost-benefit analysis to determine whether the benefit of disclosure to prevent further incidences of identity theft is worth the cost of foregoing some privacy rights that she might have. However, an alternative, or perhaps a last resort, would be to turn to the courts pursuant to § 1681b(1). This section states that if the intermediary parties disclose to a court that someone has been a victim of identity theft, then the court should be able to allow the agency to release the victim's information to other intermediary agencies. While using this approach presents several problems, such as determining which court has jurisdiction, and involving the courts at such an early stage in the process (as soon as a questionable incident occurs), it is still an option available to limit privacy concerns. Moreover, a court order can be particularly helpful if a victim cannot be located, but it is clear that an identity thief is abusing the victim's personal information and records.

agencies will infringe on her privacy rights, then the victim can refuse to have the other agencies contacted, and assume the burden of clearing her name by herself.

The database established for identity theft victims in California[231] seems to implement a link between the intermediary parties.[232] California requires its Department of Justice to maintain a database of identity theft victims,[233] but the law only allows limited access to the database for identity theft victims, criminal justice agencies, and "individuals and agencies authorized by the victim."[234] Furthermore, the law does not specify how intermediary parties become informed of the need to access the information.

Under the California law, intermediary parties may discover the need to access the database in two ways, neither of which is effective to prevent proliferation of identity theft. First, as long as the victim authorizes the Department of Justice to disclose the information, the information can be disclosed to any "individuals and agencies authorized by the victims."[235] The problem is that victims are often unaware that their identity has been stolen or that their personal identification is being used for multiple purposes.[236] Therefore, a victim will almost certainly be unaware of the need to authorize the state's Department of Justice to contact other parties, or which parties should be notified.[237]

---

[231] CAL. PENAL CODE § 530.7 (West Supp. 2003).

[232] The Idaho law also had provisions addressing the intermediary parties. *See* IDAHO CODE § [28-51-102] 28-50-102(1) (Michie Supp. 2003). However, the Idaho law only states that if a victim provides a "certified copy of a police report" to a consumer reporting agency stating that he has been a victim of the state identity theft law, the agency must "permanently block or decline to block reporting any information that the consumer identifies on his or her credit report is the result of a violation of [the identity theft law] . . . ." *Id.*

[233] CAL. PENAL CODE § 530.7(c). In order for a victim to be included in this database, the victim must provide the Department of Justice a "court order obtained pursuant to any provision of law, a full set of fingerprints, and any other information prescribed by the department." *Id.* § 530.7(a). Once the Department of Justice receives the victim's information, the information must be verified against "any driver's license or other identification record maintained by the Department of Motor Vehicle." *Id.* § 530.7(b).

[234] *Id.* § 530.7(c).

[235] *Id.*

[236] *See supra* note 53 and accompanying text.

[237] For example, if a victim learns that she has become a victim of financial identity theft, the victim may be unaware that criminal record identity theft even exists. Without being aware of the various forms of identity theft, the victim may not know who to contact, or even appreciate the need to do so. Unfortunately, the victim will likely learn all about identity theft the hard way, when she attempts to clear her credit, criminal, and/or driving records. However, the Department of Justice is aware of the intermediary parties that should be contacted. Moreover, the Department of Justice is better situated because if an intermediary party received a call from the California Department of Justice regarding identity theft, the call would likely carry more credence and be taken more seriously than a call from the

Second, criminal justice agencies may access the database at their discretion.[238] However, the agencies will only access the database if they are aware of the need to do so.[239] But when a victim enters herself into the identity theft database, only the victim and the Department of Justice are aware of the entry.[240] With the victim unaware of the need to contact other intermediary parties, or which parties to contact, the Department of Justice is better situated to make the disclosure for the victim. Thus, requiring the Department of Justice to notify other intermediary parties once a victim voluntarily enters the database would better help prevent criminal record identity theft and would alleviate some of the burden that usually falls on the victim.[241]

---

victim herself.

[238] The California statute states:

> The Department of Justice shall establish and maintain a data base of individuals who have been victims of identity theft. The Department shall provide a victim of identity theft or his or her authorized representative access to the data base in order to establish that the individual has been a victim of identity theft. Access to the data base shall be limited to criminal justice agencies, victims of identity theft, and individuals and agencies authorized by the victims.

CAL. PENAL CODE § 530.7(c). The plain reading of the statute seems to imply that criminal justice agencies can access the database without the victim's authorization. If criminal justice agencies needed the victim's authorization then it would be redundant to say that "[a]ccess to the data base shall be limited to *criminal justice agencies . . . and individual agencies authorized by the victim.*" *Id.* (emphasis added). Assuming that the criminal justice agencies can access the database without the victim's prior authorization, then the Department of Justice should notify the criminal justice agencies immediately upon the victim's entry into the database. If the criminal justice agency has already been notified by the Department of Justice, then if that person (identity thief or victim using the same information) is stopped for a traffic violation or arrested for a crime, it should send up a red flag indicating that the individual pulled over or arrested may not be the person the identity thief claims to be. If the criminal justice agency is not notified, then an identity thief who is stopped for a traffic violation or arrested for some other crime will go undetected when the thief provides the personal information of the victim. Only subsequently when the victim goes to renew her license, perhaps years after the incidents have occurred, will the victim discover the erroneous violations and be left with the burden of clearing her name or record. But if the agencies were notified ahead of time, then the identity thief can be caught and it will save the victim a great deal of time and aggravation.

[239] The likely reason that a criminal justice agency would access the database would be for a victim of criminal record identity theft who is seeking to have her record cleared pursuant to CAL. PENAL CODE § 530.5(c).

[240] Obviously, other parties could be aware of this as well; for example, the victim may tell a family member or a friend. However, the point is that while the criminal justice agency may legally have access to the database, the agency may not be aware of the need to use that access immediately.

[241] Creating a link between the intermediary parties may seem to raise some privacy issues. See *supra* note 230 for a further discussion of these privacy issues. However, there are two possible explanations for why requiring the Department of Justice to contact the intermediary parties would not infringe on privacy rights. First, the California law allows

B. INCREASE THE USE OF BIOMETRIC DATA

Increasing the use of biometric data can also help prevent criminal record identity theft. The use of biometric data refers to "the techniques and methods used to identify individuals based on a physical characteristic or particular trait unique to that individual."[242] Biometric data includes fingerprints, retina scans, iris scans,[243] hand imaging, voice recognition, and many other personal physical attributes.[244] In fact, several state identity theft laws now expressly include biometric data in the definition of personal identification information.[245]

---

criminal justice agencies to access the database without the victim's prior authorization. *See supra* note 238 and accompanying text. Therefore, the statute already grants the criminal justice agencies unrestricted access to the database. All the Department of Justice would be doing is notifying those agencies when it would be appropriate to invoke their right to access the database to retrieve information. Second, the California law is unique because the entire process of helping the identity theft victim stems from the victim voluntarily choosing to enter the database, and even providing the Department of Justice with a "full set of fingerprints." CAL. PENAL CODE § 530.7(a). Thus, the victim is choosing to enter the database so that the Department of Justice may assist her. If the victim voluntarily chooses to enter the database for assistance, and is aware of the ramifications of doing so, which are provided in the statute, the victim seems to be consenting to the other agencies accessing the database. However, it is important to reiterate that the California law, setting up a database for identity theft victims, is unique. A state that does not wish to set up such a database would seem to need the victim's authorization before disclosing any information to intermediary parties. *See supra* note 230 and accompanying text.

[242] Lisa Jane McGuire, Comment, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441, 444 (2000).

[243] For a description of why iris scans are a particularly good type of biometric data to use for security purposes see *Seeing Eye to Eye with Credit Card Users*, AUSTRALIAN FIN. REV., Nov. 28, 2001, at 8-9 (stating that the chance of two iris patterns being identical is one in ten to the power of seventy-eight, iris patterns are not determined genetically—even identical twins have different iris patterns, the iris can be detected through sunglasses, contact lenses, and even protective face plates, and in 2.75 million iris scan tests using camera recognition, there were no false readings).

[244] McGuire, *supra* note 242, at 447-48.

[245] *See, e.g.*, FLA. STAT. ANN. § 817.568(1)(f)(2) (West 2002 & Supp. 2003) ("'Personal identification information' means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any: . . . [u]nique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation."); KY. REV. STAT. ANN. § 514.160(1) (Michie Supp. 2003); N.Y. PENAL LAW § 190.77(1) (Consol. Supp. 2003); TEX. PENAL CODE ANN. § 32.51(a)(1)(B) (Vernon 2001 & Supp. 2004) ("(1) 'Identifying information' means information that alone or in conjunction with other information identifies an individual, including an individual's: . . . (B) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image.").

Biometric data is currently being used in grocery stores, workplaces, banks,[246] and airports plan to use similar methods to improve security.[247] Furthermore, because devices needed to scan biometric data are becoming more common and readily available, some predict that these devices will soon be installed on personal computers to better enhance security.[248]

Increasing the use of biometric data can be particularly helpful to prevent criminal record identity theft. Frequently, the identity thief obtains a false driver's license or other means of identification in the victim's name and gives that identification to law enforcement officials when stopped for a traffic violation or arrested for a misdemeanor.[249] In many instances, the offender signs the citation using the victim's name and promises to make an appearance in court.[250] The imposter then fails to appear in court, and an arrest warrant may be issued for the victim rather than the offender.[251] In most of these cases, no fingerprints or photographs of the wrongdoer are required.[252] However, in other cases,[253] the identity thief will appear in court for the violation and plead guilty in the victim's name, without the victim knowing that a crime is being reported in her name.[254] And in some situations, the imposter may be arrested and even taken to the county jail.[255]

---

[246] *See, e.g.*, L.A. Lorek, *Pay by Fingerprint; New Checkout Technology Lets Consumers Buy Groceries with the Touch of Their Index Finger*, SAN ANTONIO EXPRESS-NEWS, Sept. 4, 2002, at 1A (stating that fingerprints linked to a credit card or bank account are being used in some grocery stores in place of a debit or credit card, and that biometric data is also used to ensure the accuracy of employees punching in and out on time clocks at work).

[247] Frank James, *Border Control System Targets 9/11 Flaw; Visa Holders Will Get Closer Scrutiny*, CHI. TRIB., Oct. 29, 2003, at C16 (reporting that O'Hare Airport intends to use biometric data to better patrol foreigners attempting to enter the country).

[248] *See* Lorek, *supra* note 246, at 1A (claiming that some analysts believe that within the next year, devices that read fingerprints will be "routinely built into computer keyboards" for authentication purposes).

[249] FOLEY ET AL., *supra* note 8. In cases involving minor traffic violations or misdemeanors such as shoplifting, law enforcement officials do not require anything more than a driver's license, and the imposter is usually not required to go to the police station. *Id.* The imposter is only given a ticket for the traffic violation or misdemeanor and is released from arrest. *Id.* Thus, the identity thief may commit multiple crimes once the thief obtains a false driver's license in the victim's name without any violation being reported on the true offender's record.

[250] *Id.*

[251] *Id.*

[252] *Id.*

[253] *See supra* notes 1-7 and accompanying text.

[254] FOLEY ET AL., *supra* note 8.

[255] *Id.* These situations usually involve more serious violations such as felonies, drunk driving, or other public offenses. *Id.* The identity thief then provides the name and personal information of the victim. *Id.* The victim's "information is then recorded in the countywide database and is usually transferred to the State's criminal records database and possibly to

Identity theft continues to be the fastest growing crime in America,[256] and law enforcement is constantly being challenged to fight the crime effectively. With identity thieves continuously finding new ways to carry out their crime, law enforcement must devise new ways to stop and prevent the identity thieves before they act.[257] Therefore, just as biometric data is being used to ensure security in various settings, similar techniques can be used by law enforcement to crack down on criminal record identity theft.[258] If these devices are small enough to be installed at check-out counters, convenient enough to be used by workers punching in and out on time clocks, and inexpensive enough that within the next year they will routinely be attached to personal computers, then law enforcement should be able to

---

the national databases, the National Crime Information Center (NCIC)." *Id.* It is important to note that the source does not specifically say whether cases of serious violations require the suspect to be fingerprinted or photographed. On the one hand, if the imposter is fingerprinted and photographed then when the victim attempts to have her erroneous criminal record cleared she will be able to prove that her fingerprints do not match the fingerprints of the imposter, or that the name does not match the photograph or the fingerprint. On the other hand, the victim's name will be entered into a database with an erroneous photograph or fingerprint which could add to the already daunting task of having a name or record cleared. *See, e.g.*, Klein, *supra* note 9, at 1A.

[256] *See supra* note 18 and accompanying text.

[257] *See, e.g.*, Hoar, *supra* note 24, at 1427-28.

[258] The use of biometric data to stop, prevent, and catch identity theft may raise some privacy concerns. For a detailed discussion of biometric data and related privacy issues, see McGuire, *supra* note 242. However, I am not persuaded that the use of biometric data to verify personal identification information when making a traffic stop or issuing a citation for a violation of the law encroaches on privacy interests. The main reason why criminal record identity theft is a problem is that identity thieves are using the victim's identity to "evade legal sanctions" and shield themselves from criminal liability. FTC (FIGURES AND TRENDS 2001), *supra* note 12, at 4. The officer requesting the imposter's identification (such as a driver's license) is doing so only to identify the imposter. But if the identity thief is using a piece of identification in the victim's name, then providing a driver's license or other false piece of identification does nothing to assist the officer in determining who committed the traffic violation or other crime. Because biometric data is not easily stolen or reproducible, the data would seem to provide law enforcement only with the information that they were seeking in the first place, an accurate verification of the imposter's identity. *See, e.g.*, *Seeing Eye to Eye with Credit Card Users*, *supra* note 243, at 8-9. Moreover, whatever limits are in place to strike the proper balance between the need for security at airports, buildings, and workplaces and the individual's right to privacy, the same limits could be imposed on the use of biometric data to prevent identity theft. Furthermore, in the building security and employment contexts, biometric data is being used even where the person being scanned has done nothing wrong and is not subject to criminal liability. However, in the case of identity theft, biometric data would only be used in the case of an alleged wrongdoing such as a traffic violation or other crime for the limited purpose of verifying the identity of the suspect. *See* McGuire, *supra* note 242, at 473-74 (stating that if the biometric data is used only for identification purposes and not kept in a database where it can be accessed by outside hackers then there is no privacy issue).

employ similar techniques when making routine traffic stops or issuing misdemeanor citations.

V. CONCLUSION

Criminal record identity theft is a specific form of identity theft whose popularity continues to rise.[259] While many similarities exist between criminal record and other forms of identity theft,[260] criminal record identity theft presents victims with several unique problems not associated with other forms of identity theft.[261]

Although identity theft is a federal felony[262] as well as a crime in almost every state,[263] most identity theft prosecutions occur only at the state level.[264] The state identity theft laws can be divided into three general categories. First, some states have very narrow identity theft statutes only criminalizing identity theft for financial purposes.[265] The second category of statutes criminalizes identity theft for financial purposes as well as for "any unlawful activity."[266] Finally, some state laws have provisions addressing criminal record identity theft directly.[267]

Beyond these general classifications, each statute is unique, and the way in which the state laws address criminal record identity theft raises various issues. These issues include variation in penalties within a single state and across different states,[268] the penalty for repeat offenders,[269] and how to better assist victims by building methods into the laws to alleviate the victim's burden.[270] Furthermore, some states address the difficulty of finding the appropriate venue to prosecute an identity thief.[271]

However, almost all of the state laws fail to address two important issues related to criminal record identity theft. Because it takes the average victim more than a year before learning that she has been victimized, it is unclear when the statute of limitations begins to run.[272] Moreover, since

---

[259] *See supra* note 9 and accompanying text.
[260] *See supra* notes 46-82 and accompanying text.
[261] *See supra* notes 72-82 and accompanying text.
[262] *See supra* notes 92-93 and accompanying text.
[263] *See supra* notes 96-09 and accompanying text.
[264] *See supra* notes 88-90 and accompanying text.
[265] *See supra* notes 102-04 and accompanying text.
[266] *See supra* notes 105-06 and accompanying text.
[267] *See supra* notes 107-09 and accompanying text.
[268] *See supra* notes 112-29 and accompanying text.
[269] *See supra* notes 130-46 and accompanying text.
[270] *See supra* notes 147-57 and accompanying text.
[271] *See supra* notes 158-62 and accompanying text.
[272] *See supra* notes 171-81 and accompanying text.

most identity theft statutes are relatively new, the statute of limitations issue is bound to arise in the future. Unless the states address this problem, the current statutes seem ill-equipped to handle the issue properly.[273] Second, the state identity theft laws fail to address the reverse criminal record identity theft problem.[274] Thus, looking at the state identity theft laws collectively, one can suggest the necessary provisions that a comprehensive state identity theft statute would include.[275]

Criminal record identity theft can be better controlled and prevented in two ways. First, because the victim does not always become aware that she has become a victim of identity theft immediately, there should be a direct link between the intermediary parties that are in between the victim and the thief.[276] Creating this link will help prevent identity thieves from using the victim's information for multiple forms of identity theft. Additionally, this link will assist the victim by shifting some of the victim's burden of clearing her name and record to the intermediary parties.[277]

Finally, increasing the use of biometric data can help minimize criminal record identity theft directly.[278] Small devices to read fingerprints, retina scans, and other forms of biometric data are already being used in a variety of settings to ensure security.[279] Similar devices could be used by law enforcement when making routine traffic stops or other arrests that do not usually require fingerprints or photographs.[280] The use of biometric data will ensure that the perpetrator of the crime is actually who she claims to be.

With identity theft at its highest level and continuously growing, states must consider amending their laws to better address criminal record identity theft and the problems associated with it.

---

[273] *See supra* notes 182-89 and accompanying text.

[274] *See supra* notes 190-202 and accompanying text.

[275] *See supra* notes 203-15 and accompanying text.

[276] *See supra* notes 221-41 and accompanying text.

[277] *See supra* notes 74-79 and accompanying text.

[278] *See supra* notes 242-58 and accompanying text.

[279] *See supra* notes 246-48 and accompanying text.

[280] *See supra* notes 249-55 and accompanying text.