NORTH-HOLLAND

Financial Services Review 10 (2001) 221–235

FINANCIAL SERVICES REVIEW

Identity theft: no help for consumers

John E. Matejkovic*, Karen Eilers Lahey[1]

Department of Finance, College of Business Administration, University of Akron, Akron, OH 44325-4803, USA

Received 1 November 2001; received in revised form 20 November 2001; accepted 13 December 2001

Abstract

Identity theft is a growing problem in the American economy. While there have been attempts to address and minimize the problem, those attempts have focused on making identity theft a crime. This paper discusses the inadequacy of this approach from the perspective of individual victims of identity theft, and the fact that the law currently provides those victims little recourse or remedy for the harms they suffer. It also offers a proposal for legislation that would provide some remedy as well as an incentive to protect consumer identity information. © 2001 Elsevier Science Inc. All rights reserved.

JEL classification: G21; G28; K23; K42

Keywords: Identity theft; Identity fraud

1. Introduction

The stories demonstrate how prevalent the problem is, and how easy a crime it is to commit. What they don't report, too often, is how little help is available to consumers who have been victimized.

For Dongwei Su, it was as simple as using information from a credit card statement that had been mailed to a prior resident at his address, taking information from a roommate's wallet, and looking at a fellow student's driver's license. By the time authorities caught up with him, he had used other peoples' credit to obtain more than $115,000 worth of goods and services (Caniglia, 2001).

Lynda Davidson, aka Lynda London, got hired as a paralegal, and then used one of her bosses' identities to obtain a cell phone. The same boss became concerned when creditors started calling the office regarding loan applications and loans, involving names and social security numbers of the firms' clients. After reading of Davidson/London's arrest, another

* Corresponding author. Tel.: +1-330-972-8243; fax: +1-330-972-5970.

E-mail addresses: jem@uakron.edu (J.E. Matejkovic), klahey@uakron.edu (K.E. Lahey).

[1] Tel.: +1-330-972-5436.

PII: S1057-0810(02)00089-6

lawyer reported Davidson/London's employment with him, and discovered that she had used eight social security numbers, and four other names, and had outstanding arrest warrants in several states (King, 1999).

Lamar Christian downloaded the names and social security numbers of hundreds of U.S. military officers from a Web site, and then opened credit accounts with First U.S.A. Bank Online, then used those accounts to obtain approximately $161,000 worth of merchandise (Consumer Financial Services, 2000). Sherri Samantha Bius stole mail from mailboxes, drop boxes, and post offices. She used the information from the stolen mail to not only access current accounts, but to also create new accounts and to cash stolen checks (Nat'l Assn. Attorneys General, 2000).

The problem is identity theft, which is defined as the obtaining and use of another individual's personal identifying information such as names, birth dates, social security numbers, etc., to obtain access to that individual's accounts or credit, or to establish new accounts or credit in the victim's name, without the victim's involvement or knowledge, and the use of those accounts and/or credit to obtain goods and/or services. The problem of identity theft is rather pervasive and widely reported. What is not as widely reported is the lack of protection and adequate remedy available to those individuals who are victims.

Identity theft has been described as "The" crime of the information age. Some data exists to indicate that one in four adults has been the victim of some type of identity theft, with the U.S. Public Interest Group estimating that 40,000 people are victims of such activity each year. One law enforcement official states: "... identity assumption and takeover is becoming the most serious non-violent crime ... that America faces" (Ivey, 2000). Some media report 700,000 cases of identity theft yearly (Foley, 2000).

The focus of this paper is the economic aspect of the problem, and the lack of protection and remedy for victims. But, as is demonstrated herein, the variety of forms that identity theft can take has been one of the main impediments to reducing the incidence of such thefts, and providing individual victims viable remedies for their injuries.

2. The magnitude of identity theft

In response to a request from members of Congress, the United States General Accounting Office (GAO) prepared a briefing and summary report entitled "Identity Fraud. Information on Prevalence, Cost, and Internet Impact is Limited" (1998). The GAO report represents the most consistent, reliable information on the impact, economically, of identity theft. The GAO gathered information from various Federal agencies and offices, including the Federal Bureau of Investigation, the Secret Service, the Internal Revenue Service, the Federal Trade Commission, and others. It also obtained information from the three major credit-reporting agencies (Equifax, Experian, and TransUnion), major credit-card companies, and various other constituencies.

Officials at VISA U.S.A., Inc. and MasterCard International, Inc. indicated overall fraud losses to member banks in the hundreds of millions of dollars. MasterCard reported losses of $407 million in 1997, with 96% of those losses attributed to identity fraud. According to the U.S. Secret Service actual losses to individual victims and institutional victims increased

from $442 million in fiscal year 1995, to $450 million in 1996, to $745 million in 1997. An official with TransUnion Corp., one of the three main credit reporting agencies, estimated that two-thirds of all consumer calls to the company's Fraud Victim Assistance Department involved identity fraud, and that the numbers of inquiries increased from 35,235 in calendar year 1992 to 522,922 in 1997.

VISA U.S.A. noted that within the credit card industry there was no standard definition of identity fraud, but advised that in 1997, member banks' fraud losses totaled $490 million. Five percent of those losses were "fraudulent applications" (being most closely involving identity fraud), with another 6% of those losses being "account takeovers" (which includes mail theft). Despite the millions of dollars involved, the losses represented 0.097% of VISA U.S.A.'s business volume, and only 0.11% of MasterCard's volume.

Beyond the mere recitation of data, however, the GAO report is noteworthy in that it points out some of the problems in not only tracking identity theft and its costs, but in calculating what those costs are.

> Identity fraud may be an element in a variety of financial crimes. No Federal agency has overall primary jurisdiction for the investigation of such fraud. Identity fraud is difficult to track because there is no standardized definition. Also, the scope or types of identity fraud can range from unauthorized use of a credit card to a total takeover of a person's identity (GAO, 1998, p. 2).
>
> On the individual level, the "human" costs of identity fraud should be acknowledged. Emotional costs are associated with identity-fraud incidents as well as the time and effort required to repair a compromised credit-history. One Secret Service field agent told us that victims of identity fraud feel they have been violated. Although not easily quantified, the financial and/or opportunity costs to victims can also be substantial. For example, the victims may be unable to obtain a job, purchase a car, or qualify for a mortgage (GAO, 1998, p. 49).

Yet, even when the victim's costs can be quantified, they still may have no effective remedy.

One of the requirements of the Identity Theft and Assumption Deterrence Act, 1998 (18 U.S.C. §1028, Pub. Law 105-318, 112 Stat. 3007), is that the Federal Trade Commission (FTC) establish procedures to keep track of consumer complaints of identity theft, provide victims with informational materials, and refer the victims' complaints to appropriate law enforcement and consumer reporting agencies. As a result, on November 1, 1999, the FTC established the Identity Theft Hotline and Data Clearinghouse. Between the date of inception of the Hotline and June 30, 2001 the FTC logged over 97,000 entries, increasing from an average of 445 calls per week in November 1999 to over 1800 calls per week in June 2001.

The most common forms of identity theft reported to the Hotline were: credit card fraud (43%); unauthorized phone or utility services (21%); bank fraud (14%); fraudulent loans (7%); government documents or benefits (7%); and other identity theft. This last category includes misuse of the victim's identity to gain employment, obtain medical services, evade law enforcement, declare bankruptcy, lease property, and open or access Internet accounts.

The average time between the identity theft and the date of discovery was 12 months, but 45% of the victims discovered the theft within 1 month. The report notes that "... some of

the victims were unaware of the theft for as long as 5 years'' (FTC, 2001, p. 4). Perhaps as a result of the increased publicity and public awareness of the problem, 64% of the callers had already contacted credit bureaus, and 97% of those had placed ''Fraud Alerts'' on their files. Of interest is the fact that when a caller reported that they had contacted local police, in only 72% of those contacts was a police report generated. Yet, despite the recognition of the various problems, a victim of identity theft may encounter, there is still no adequate remedy available to them for such problems.

3. Criminalization of identity theft

Certain aspects of identity theft have long been criminal activities. Part of the problem with tracking the various incidents is that they also usually are part of some other criminal activity. There have long been statutes prohibiting activities that we describe and discuss herein as identity theft, at both the Federal and State level (18 U.S.C. §1344 (bank fraud), 18 U.S.C. §1341 (mail fraud)), and therefore tracking information about such thefts, and passing legislation to cover all aspects of such thefts has often been problematic. When the question is asked: ''Isn't credit card fraud already illegal?'', the answer must be: ''Yes, but . . .''. Merely criminalizing certain aspects of identity theft hasn't provided sanctions for all aspects of such a theft, nor has criminalization provided victims of the identity theft with adequate protection of their interests.

3.1. State actions and legislation

Responding to the pervasiveness of the problem of identity theft, and often to ''plug holes'' in their criminal statutes, many states have adopted laws that criminalize the act of assuming or using another person's identity. While an examination or survey of all of the various state statutes is beyond the scope and purpose of this discussion, some examination of the states' reactions is appropriate, if only to demonstrate that mere criminalization is inadequate to provide consumers with more adequate protection.

For the most part, the states' reactions have been to adopt statutes that penalize the possession or use of identifying information for a variety of stated purposes. They range from the very simple in approach to more complicated schemes designed to provide consumers protections and resources beyond the mere prohibitions and penalties.

As an example of a simpler approach, Ohio Revised Code §2913.49 makes it a first degree misdemeanor to merely ''[O]btain, possess or use any personal identifying information of any living or dead individual with the intent to fraudulently obtain credit, property, or services or avoid the payment of a debt or any other legal obligation''. Personal identifying information is very broadly defined to include name, address, telephone number, driver's license and/or driver's license number, social security card and number, place of employment and/or employee identity numbers, mother's maiden name (probably the most frequently used ''safeguard'' information), financial institution account numbers and PINs and passwords, and credit card numbers. It also prohibits aiding and abetting, and the creation of such information for the purpose of aiding and abetting. If the violation is part of

a course of conduct (i.e., there are several identities involved or one identity is misused for a variety of improper purposes) a court is permitted to aggregate all of the amounts of credit, property and services obtained for purposes of sentencing. As appears to be the norm for most state enactments, and in accord with other criminal offenses, the level of criminal sanction escalates according to the value of credit, goods, or services obtained. If the value of credit, goods, or services obtained is $100,000 or more, the criminal offense is a third degree felony (a middle level of criminal sanction, which normally involves a number of years of imprisonment along with substantial fines).

Some states have proposed legislation than not only criminalizes an identity theft, but also adds additional protection for consumers. An example of this approach is Idaho Attorney General Al Lance's package of different laws, which include prohibitions against misrepresenting an identity via E-mail, prohibiting disclosure of adverse credit information that resulted from an identity theft, and a requirement that personal financial information not be sold without the consumer's written prior authorization (Idaho Code §28-51-101).

At the other end of the criminalization/regulatory spectrum, are those enactments in the State of California, which in 1997 became the second state to make identity theft a criminal offense; a misdemeanor at first, but subsequently amended to escalate the offense in some instances to a felony, with fines of up to $10,000 and/or imprisonment. In addition, a victim of identity theft can petition a court to be found factually innocent of any crime committed by an identity thief using the victim's identity, and to even expunge that arrest and conviction. More recently, California enacted additional statutory provisions designed to provide additional help and protection to persons victimized by identity thieves.

Under California law (Penal Code 530.6), "A person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another ... may initiate a law enforcement investigation by contacting the local law enforcement agency that has jurisdiction over his or her actual residence, which shall take a report of the matter ... and begin an investigation of the facts ...". Under this provision, a victim of identity theft may petition "a court" for a finding of factual innocence applicable to that victim, and the court "shall issue" an order certifying this determination, if the court it to be correct. Moreover, the Judicial Council of California is to develop a uniform order for the courts to use in issuing such orders. If such a finding is later found to be the result of any material misrepresentation or fraud, the court maintains the power to vacate the determination.

California Penal Code 530.7(c) requires the establishment of a database accessible by victims and others authorized, establishing the individual's status as a victim of identity theft. To be included in this database, a victim is required to submit proof of their identity by means of a full set of fingerprints, and any other information prescribed by the department.

The intent behind these recent enactments is to provide victims, a readily accessible reference and resource to establish their status. This would, presumably, make it easier for them to establish who they are and what they have, or have not, done in any given circumstance. Supposedly, they would have a much easier time clearing up a credit history or record, and avoiding any liability for an unlawfully established debt or account by use of this registration. Similarly, should a victim of identity theft have an encounter with a law enforcement agency due to a misuse of that victim's identity (i.e., the thief having an outstanding warrant, or an arrest record using the victim's identity), it should be easier for

the victim to avoid any unnecessary delay or involvement with that law enforcement agency. Despite the breadth of the California scheme, and the attempted protections sought for victims of identity theft, some commentators note certain weaknesses (Stanley, 2001).

3.2. The Federal Identity Theft and Assumption Deterrence Act, 1998 (18 U.S.C.§1028, Pub. Law 105-318, 112 Stat. 3007)

In 1997, Senate Bill 512 was introduced by Senator John Kyl (R-Arizona). A parallel measure was introduced as House bill H.R. 4151. Known as the Identity Theft and Assumption Deterrence Act, 1998, it was passed by Congress and signed by President Clinton on October 30, 1998, with an effective date of January 1999. The Act amended certain portions of chapter 47 of Title 18 of the United States Code, establishing the Federal crime of identity theft, establishing definitions, and penalties for violation of the Act, and establishing certain non-criminal requirements, such as the establishment of the FTC's Clearinghouse (18 U.S.C. §1028, Pub. Law 105-318, 112 Stat. 3007).

While there are several other provisions of the U.S. Code penalizing various activities that are usually facets of identity theft, the Act accomplished a number of things. First, it classified victims of identity theft as victims of this particular crime, whereas victims had previously been viewed merely as 'secondary' victims, with any defrauded financial institutions, etc., being viewed as the primary victims of such a theft. Secondly, it Federalized the crime of identity theft, allowing victims the aid of law enforcement officials when the perpetrator of the theft may have never even set foot in the victim's state of residence. Thirdly, and perhaps most importantly, it made the mere theft of someone's identity a crime, in and of itself, even if no other provisions of the U.S. Code were violated.

The Act states that an identity theft is committed by anyone who ''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''. A means of identification includes such things as an individuals name, social security number, date of birth, biometric data such as fingerprints, and electronic and telecommunications codes. The Act further instructed the U.S. Sentencing Commission to amend the U.S. Sentencing Guidelines, taking into consideration such things as the number of victims involved, the number of identification documents used by the perpetrator, the amount of loss involved, the difficulty and/or damage done to the victim's reputation and restoration of their reputation, and to generally incorporate the concept of identity theft into relevant fraud related Guidelines. It is given a fair amount of discretion as to what may be considered (28 U.S.C. §994 note). Criminal sanctions include fines and imprisonment, with sentences ranging from three years up to 25 years if the identity theft also involved drug trafficking or violence, or if the perpetrator has a prior conviction (18 U.S.C. §1028(b) (3) and (4)).

In Section 5 of the Act, Congress instructed the FTC to log and acknowledge receipt of complaints from individuals who either had, or reasonably believed they had, been victims of identity theft, provide informational materials to those victims, and refer those individuals to ''appropriate entities'' (including the three main consumer credit reporting agencies). This is the genesis of the FTC Clearinghouse.

In adopting the Act, Congress accomplished two significant goals: the Federalization of, and recognition of, identity theft, as a crime in and of itself; and the establishment of a centralized source of information for victims and law enforcement personnel (and others) to obtain and record accurate data regarding aspects of the crime. However, despite the recognition afforded, and the rather stiff penalties available in cases of identity theft, the Act still does not provide consumer victims adequate protection and remedies.

4. The inadequacy of criminalization

As discussed, the primary Federal response to the problem of identity theft has been to define it as a Federal crime and provide criminal sanctions for its violation. Interestingly enough, however, the final version of the Act specifically excluded provisions contained in a proposed version that would have aided victims of the crime by providing restitution of the costs associated with restoring their credit histories, and clearing up problems caused by identity theft. As originally introduced, S.B.512 contained provisions allowing Federal courts to award restitution to individuals who incurred expenses as a result of their identities being stolen. The House Bill did not contain such provisions, and they were absent from the version adopted. Only ''direct'' victims of the crime (such as financial institutions) can be awarded such restitution as having been ''proximately harmed'' (18 U.S.C. §3663(a) (2)). The failure to include such provisions continues the perception that victims of identity theft have often encountered, that they are not the ''true'' victims of the crime; that the ''true'' victims are those credit card companies and other financial institutions that have extended credit, or made loans to the perpetrators of the theft. And it should be conceded that in terms of sheer volume (i.e., total dollar cost/losses) financial institutions are the main ''victims'' of identity theft; but, as indicated above, that volume of losses represents a very small percentage of an institution's business.

And it certainly is true that in some instances an individual victim has certain protection, even if by means of a limited liability, when an identity thief makes use of an existing account. The best example might be under the Truth-in-Lending Act, as amended, which limits an individual account holder's liability to $50 for use of a lost or misused credit card (or zero liability, if a lost card is reported prior to it's being used) (15 U.S.C. §1643). Similarly, under the Fair Credit Billing Act, and individual has the right to dispute charges that appear on a credit card statement, and have any collection action(s), interest charges, etc., in respect to such disputed items held in abeyance pending investigation and resolution of those disputes (15 U.S.C. §1681). Thus, it could easily be argued that an individual victim of identity theft is not even the ''main'' victim of the theft; the major portion of any economic loss would be borne by a financial institution.

As noted, many victims could not even get local police and law enforcement agencies to even make a report of the theft. Yet the perception ignores the many instances where victims of identity theft have expended hundreds, or even thousands of dollars to either correct their credit histories, or defend themselves from actions taken to collect debts incurred by perpetrators who have stolen and/or assumed the victims identities. A review of some of the cases involving identity theft clearly demonstrates the inadequacy of the current state of the law.

4.1. Mattly v. Spiegel Inc. (2000) (19 S.W.3d 890 (Tex. App.))

Diane Mattly was a victim of identity theft who was almost further victimized by a financial institution that had been victimized by the perpetrators of Mattly's identity theft. Over 18 credit cards had been opened by the perpetrators, and Mattly did one of the things that all victims of the identity theft are advised to do: she contacted credit reporting agencies to report the theft, and have a ''flag'' placed on her report. The ''flag'' would alert credit agencies, and credit extenders, that Mattly was a victim of identity theft, and no new accounts should be opened until her identity was verified.

After her report had been ''flagged'', and supposedly in response to a ''pre-approved'' card offer that was mailed to Mattly's home, Spiegel opened an account in Mattly's name, which was used to charge over $2,000 worth of merchandise. Mattly eventually hired an attorney and investigator to help her clear her account with Spiegel, who had turned the account for collection with FCNB. On the advice of her attorney, Mattly filed suit against Spiegel and FCNB, claiming Spiegel was negligent in opening the disputed account, and had also violated the Fair Credit Reporting Act. The sole damages Mattly claimed were the attorneys' fees she incurred in clearing up the disputed account, and incurred in prosecuting her suit against Spiegel. Spiegel and FCNB denied Mattly's allegations, and counter sued Mattly, claiming that Mattly's claims were brought in bad faith. After the suit had been pending for a year, Mattly dismissed her claims, because the case had become too expensive, noting that she had incurred over $14,000 in attorneys' fees to the point of her dismissal. Subsequent to Mattly's dismissal, the trial court awarded sanctions against Mattly and her attorney in the amount of $5,000.

On appeal, the judgment for sanctions was reversed. The appellate court noted that Mattly's dismissal was not because of some bad faith or malice—it was because Mattly couldn't afford to continue the suit. Similarly, since she had consulted with two attorneys who felt she had a valid claim, Mattly's initial filing was not found to be a bad faith or malicious act, even when the only damages when sought was recovery of the attorney fees she had expended to settle her dispute with Spiegel, since there was some argument under Texas law that attorney's fees in some instances might be recoverable items of damages. Diane Mattly may not have paid Spiegel's on a fraudulent account, but she was victimized to the tune of over $14,000, and it was nearly $20,000.

4.2. Guzman v. Toyota Motor Credit Corp. (1999) (745 So.2d 1123 (Fla. App.))

In 1985, Alejandro Guzman discovered someone had stolen his identity. The thief obtained various loans in Connecticut, and had even purchased a new Toyota, incurring a loan with Toyota Motor Credit Corp. (TMCC) for $28,672.21. Guzman spent a year and a half clearing his credit history, and was successful except for the TMCC loan. Even after Guzman reported the fraud, TMCC maintained the account as open, as for some period the identity thief kept the account current.

Eventually, the thief stopped paying, and the account went to default. Despite the fact that Guzman had notified TMCC of the fraud in 1995, when the loan defaulted in 1997, TMCC attempted to collect from Guzman, even to the point of filing suit. Four days before a

hearing on a Summary Judgment motion (presumably filed by Guzman), TMCC dismissed their suit.

Guzman then filed suit against TMCC alleging that their collection suit constituted an abuse of process and a malicious prosecution. While Guzman's initial filing also included claims against TMCC for invasion of privacy and violation of Florida's Consumer Collection Practices Act, those allegations were subsequently dropped. TMCC moved for Summary Judgment, which was granted by the trial court, noting that all TMCC's methods ''were the usual initial steps in a routine debt collection using only standard civil procedures''. ''To hold otherwise would put . . . creditors at risk in routine, noninvasive, noncriminal collection practices to attempt to locate and verify the identity of a debtor''. The Court of Appeals reversed the trial court's grant of Summary Judgment, and ordered the trial court to resolve whether or not, factually, TMCC's suit was a reasonable collection effort when no further investigation had been done, and whether or not ''. . . TMCC acted in the usual and customary manner as to the creditor in a typical collection case''.

It would be hard to argue that TMCC was not reasonable in filing of the initial collection suit against Guzman. Civil proceedings are designed to handle exactly these types of disputes and provide discovery procedures and due process guarantees to insure a fair, true and just outcome. Even with the notice that a fraud may have been committed, what was ''wrong'' about TMCC utilizing the procedures established in our judicial system to verify that Guzman was, or was not, the debtor? Surely, TMCC had filed hundreds, or thousands, of collection actions previously; and undoubtedly in some of these actions the ''it ain't me'' defense must have been raised. Why shouldn't TMCC have access to the courts, and the tools they provide, to find their debtor and collect their debt? When it appeared Guzman was not ''their man'', they dismissed. And Guzman, in addition to spending unknown hours clearing his name and credit history, was also left with a legal bill to pay for his defense from TMMC. Despite all the other protections the law may provide, Guzman was victimized again.

4.3. Polzer v. TRW Inc. (1998) (682 N.Y.S.2d 194)

Jeffrey and Kathleen Polzer had impeccable credit histories. They believe their identities were stolen when the submitted a loan application for a new car. In less than 4 months, the identity thief succeeding in changing the Polzers' addresses with their banks and all the credit reporting agencies, and ran up over $100,000 in fraudulent charges. While the Polzers closed accounts and took other steps to regain their credit history, it took a substantial time for them to escape from the morass. Credit reporting agencies sold their reports continually—with the fraudulent accounts and the thief's address; ''pre-approved'' cards were issued. Correctly deleted information was reinserted, and it took TRW over 10 months after notification to remove Polzers from pre-approved credit offer lists. It took some agencies more than 2 years to remove fraudulent account information, and to list Polzers correct address. Yet, other than the time involved, the Polzers apparently suffered no pecuniary losses.

Polzers filed suit against a number of entities, including banks (Bank of New York), credit reporting agencies (TRW, 2001), and issuers of fraudulent credit cards (Mobil). The trial

court granted motions to dismiss all of the defendants, an action which was affirmed by the Court of Appeals. The appellate court, in a very succinct opinion noted that New York did not recognize ''negligent enablement of impostor fraud'', and that any claims based on some infliction of emotional distress had to fail, as ''there was no evidence of ill will, malice, or extreme outrageous conduct'' Claims alleging violations under New York's Deceptive Acts & Practices Act were also dismissed, as there was no proof that the defendants engaged in any acts that were deceptive or misleading to plaintiffs. Polzers spent several years clearing up their credit histories as a result of an identity thief; undoubtedly hundreds of hours of time and effort, at the least, and had no remedy available for their efforts.

4.4. Patrick v. Union State Bank (1996) (681 So.2d 1364 (Ala.))

Of all the civil cases the authors found involving a civil remedy for victims of identity thieves, only one state, Alabama, has provided such a remedy. In April 1990, Bridgette Patrick applied to renew her driver's license, and received a temporary license that had no photograph. Several weeks later, Patrick noticed that the temporary license and a store credit card were missing. She reported the missing credit card, and eventually received her permanent renewal license. Months later, Patrick received a notice of an outstanding arrest warrant against her for issuing bad checks. Patrick appeared at the police station, and after her signature did not match the drawer's signature on the bad check, the charges were dismissed. This circumstance was repeated in another city.

Patrick believed that there must be another ''Bridgette Patrick''. She was wrong. In 1992, after being stopped by police for a traffic offense, Patrick spent 10 days in jails, as she was shipped from county to county to respond to arrest warrants in those locations on bad check charges. All of the charges against Patrick in 11 different jurisdictions were eventually dismissed.

All of the bad checks were drawn on Union Bank, which had opened the account when an imposter presented Patrick's stolen temporary driver's license as identification. The imposter advised the bank that the address on the license wasn't accurate, as she was living in a battered-women's shelter. The bank required no additional identification, and there were other irregularities in the opening of the account.

Patrick filed suit against Union Bank, alleging that it negligently allowed an imposter to open an account using her identity, without requiring proper identification or otherwise verifying the information provided to open the account. The trial court granted Summary Judgment to the bank, noting that plaintiff failed to establish any duty owed by the bank to plaintiff, or any proximate cause between the bank's alleged negligence and Patrick's injuries. The Alabama Supreme Court disagreed.

The Court first noted that as a general rule, liability is not imposed on one party based upon the criminal actions of another party. However, the Court noted that this principle arose out of cases involving physical assaults, which was obviously not involved in this case. Here, the Court noted, the bank became involved in a relationship with the plaintiff (Patrick) by opening an account in her name, and it was the opening of the account, not some unrelated criminal activity, which gave rise to the plaintiff's problems. Noting that it was foreseeable that opening a fraudulent account could cause an innocent victim substantial problems, the

Court then stated that the bank was in the best position to avoid or prevent the fraud which occurred. Thus, the Court held, ''the imposition of tort liability could be appropriate''.

Thus, in Alabama at least, if the primary vehicle of an identity thief is through use of a fraudulently opened bank account, a victim may have some civil remedy. However, this holding may be more limited than would appear on first blush: the Court placed some emphasis on the bank's failure to follow it's own procedures, and emphasized the forseeability of 'injury' to the plaintiff (i.e., the arrest, etc.) for passing bad checks. Had the identity thief used the fraudulent account for other purposes, or merely as a tool in some other aspect of identity theft, perhaps the result might be different. And, of course, there are many other means available to steal an individual's identity.

4.5. Andrews v. TransUnion Corp. (2001)/TRW. (7 F.Supp.2d 1056 (C.D.Calif. 1998), aff'd in part, rev'd in part, 225 F.3d 1063 (9th Cir. 2000), cert. grtd., 532 U.S. 902)

On June 17, 1993 Adelaide Andrews visited a radiologist's office in Santa Monica, California. Since it was her first visit, she was required to fill out a Patient Information Form, listing her name, address, date of birth, and driver's license and social security numbers. After completing the form, Adelaide handed the form to the doctor's receptionist: Andrea Andrews. Some time later, Andrea relocated to Las Vegas, and began using Adelaide's identity. She leased an apartment and obtained utility services using the stolen driver's license and social security numbers, and attempted to obtain credit, although she used either her first name instead of or in addition to Adelaide's in those instances. One of the attempts to obtain credit occurred when Andrea applied for a Dillard's charge card. Dillard's requested credit information from TransUnion, which passed three credit files, with an ''alert'', because of discrepancies between the information provided and the information on file. Dillard's allowed Andrea credit in Adelaide's name, and the account later went delinquent. Other attempts by Andrea to obtain credit were processed through TRW.

In May 1995, Adelaide attempted to refinance her mortgage. The financial institution (Home Savings) obtained a credit report from Chase Credit Research (a non-party to Adelaide's suit), which was prepared based upon information received from TransUnion, TRW, and Experian (also not named in the suit). That report listed the delinquent Dillard's account. Because Adelaide believed that she would not be approved for the refinance at Home State, she found alternative financing, allegedly at a higher interest rate. On June 5, 1995, Adelaide contacted TransUnion, which immediately placed a ''Fraud Alert'' flag on her credit report. On June 22, after checking with Dillard's and determining that that account was fraudulently opened using Adelaide's stolen identifiers, TransUnion suppressed the information regarding that account from her report. The report continued to show an inquiry from Dillard's on the date Andrea applied for the account, however.

On October 21, 1996 Adelaide filed suit against both TransUnion and TRW, alleging violations of the Fair Credit Reporting Act (FCRA), and a violation of California law. Adelaide claimed the defendants violated FCRA by improperly disclosing her credit report in response to the inquiries made as a result of Andrea's theft of her identifiers; failing to maintain ''maximum possible accuracy'' of the information in her report; and, that TransUnion failed to reasonably reinvestigate and promptly delete misinformation in her

report. Plaintiff sought compensatory and punitive damages for her expenditure of time and effort to clear her record, and for commercial impairment, inconvenience, embarrassment, humiliation, and emotional distress including physical manifestations (triggering of a Lupus attack). Both defendants moved for Summary Judgment on various aspects of plaintiff's claims.

Although it was subsequently amended, at the time of plaintiff's claims FCRA required credit reporting agencies to verify the identities or individuals requesting reports, and that such reports be released only for proper, established, purposes. FCRA also set forth a 2-year statute of limitations, "... except that where a defendant has materially and willfully misrepresented any information ... the action may be brought any time within 2 years after discovery ... of the misrepresentation". Since two disclosures were made more than 2 years prior to Adelaide's suit, the trial court ruled that those disclosures were not actionable. As to the disclosures made within the 2-year period, the court held that a claim could be made only if a plaintiff proved an impermissible purpose. Since Adelaide's files were released upon her apparent application for credit, the court held that those disclosures were proper. The court also noted that the credit reporting agencies had conducted proper investigations, and obtained certifications from all requestors prior to releasing any information. With regard to plaintiff's claim that her report contained inaccuracies, the Court noted that plaintiff first had to prove that the report was inaccurate, and then had to prove that the credit reporting agency's procedures were unreasonable; in an "accuracy" claim, it was not necessary to prove actual pecuniary loss. Since TransUnion supplied two reports, one showing the imposter's Dillard's delinquency, but also using Adelaide's Social Security number, the court held that a jury could find for the plaintiff on this claim, and allowed it to proceed to trial. Since Plaintiff's "reinvestigation" claim was based upon the listing of an inquiry from Dillard's, the court held that a jury should also determine if that "reinvestigation" was reasonable.

Because the claims against TRW were based on improper disclosure, plaintiff was required to prove an actual pecuniary loss. However, the court noted that plaintiff voluntarily decided not to proceed with the refinancing based upon an assumption that she would not be approved. Thus, the Court concluded that she could not prove any recurring damage caused by the alleged improper disclosure, and granted TRW a summary adjudication that TRW had not caused the plaintiff any pecuniary damage.

The case proceeded to trial, and a jury returned a verdict in favor of the defendants on the two claims still left: the "accuracy" claim, and the "reinvestigation" claim. Andrews appealed.

The Ninth Circuit Court of Appeals' decision was short and to the point. Addressing the statute of limitations issue, the Court noted, "The general Federal rule is that a Federal statute of limitations begins to run when a party knows or has reason to know that she was injured". Noting the discrepancies between the information that imposter Andrea provided and the file information about Adelaide, the court noted that the reasonableness of the disclosures was a decision best left to a jury, and thus the trial court's dismissing those claims was improper. Finding no other reversible error, the Court reversed the trial court's rulings on the "disclosure" claim, and remanded the case for a new trial. The Supreme Court granted certiorari, and in a very recent decision, ruled that the trial court had correctly

interpreted the statute of limitations issue, and that a plaintiff had only 2 years from the date of any disclosure in which to file suit based upon an alleged wrongful disclosure.

The impact of this ruling is clear: consumers had best obtain copies of their credit reports on an annual basis, or they may miss any opportunities to complain of wrongful disclosures. An additional burden has been placed on individual consumers, instead of aid in their efforts to avoid or minimize their exposure to identity theft.

5. Conclusion

There are so many instances of identity theft, and so many ways it may be accomplished. The costs and losses are significant to financial institutions and individuals, but are often difficult to determine, especially for individual consumer victims. If an individual is fortunate enough to avoid financial liability for the theft, they still suffer losses, even if those losses are ''merely'' time and effort, and are harder to quantify. Yet Alejandro Guzman and Dianne Mattly incurred substantial expenses in addition to the time they spent recovering from the theft.

Financial losses should be recoverable to the victim, from someone. But experience and common sense indicate that thieves are rarely collectible defendants, and even when courts impose restitution as part of a criminal conviction that restitution is rarely an effective remedy. Convicted criminals rarely have significant earning capacity.

Other avenues of recovery, especially tort-based theories of recovery, are also limited. The law currently recognizes no relationship between a thief and a victim. No court has yet held that a person's identity is a legally recognized property interest that can be converted. Perhaps a claim against the individual or entity that enabled the theft would seem more just, or appropriate, but the law does not normally impose liability on one person for another person's criminal activity. The law generally recognizes criminal conduct as an intervening or superseding cause, which breaks the causation chain in a negligence claim (Restatement (Second) of Torts §442). Thus, if a plaintiff claims a defendant was negligent in allowing an employee access to the plaintiff's identity information, or that a web site was negligent in posting identity information, that negligence is no longer the cause of the plaintiff's injury.

Obviously, something should be done to reduce or eliminate the problem of identity theft; and it would seem equally obvious that it is not equitable to allow individuals to be victimized by such a theft, whether their loss is quantifiable or ''merely'' the expenditure of time and effort to restore damaged credit. The authors suggest an action that would not only recognize the individual victims' losses, quantifiable or not, and provide compensation for those losses, but that would also have the desirable effect of providing an incentive to protecting personal identity information: adopting legislation that imposes strict liability on any person or entity that gathers, compiles, posts in any public or semi-public fashion, requires, transmits or uses personal identity information. The legislation should provide that liability should be imposed without a determination of fault; the only requirement would be that the source of the stolen information be identified. There should also be minimum damages awarded, or an award of quantifiable economic losses: the victim would recover actual economic losses or $2,500, whichever is greater. Economic losses would include

actual out-of-pocket costs and expenses, and would specifically include court costs and attorneys' fees in any action or activity related to the theft, as well as any court costs and attorneys' fees to collect under the legislation. Those individuals or entities that act with reckless indifference toward the security of personal identity information would be exposed to punitive damages as well. Personal identity information would be defined the same as in the Identity Theft and Assumption Deterrence Act. The legislation should be at the national/Federal level.

There is already precedence for this type of liability: in criminal law liability is imposed strictly for everything from underage sales of beer and liquor to what is commonly referred to as ''statutory rape''; in civil cases, liability without fault is imposed on sellers of defective products. Similarly, there are many instances where statutes impose maximum damages, even in the absence of actual, demonstrable loss.

Is the proposal a ''perfect'' solution? Of course not; there are many instances where the thief is never caught, and therefore the ''source'' of the stolen identity would probably not be discoverable. Where the ''source'' of the stolen information is a governmental agency, there may be constitutional or immunity issues; however, the governments involved might allow such claims to proceed in Courts of Claims established in most states. Since most cases of identity theft would appear to have been based upon information ''sourced'' for non-governmental entities, it would seem that those concerns might be limited.

The legislation would also provide strong incentive to keep identity information secure. It is doubtful that anyone would establish a web site listing names and social security numbers appreciating the exposure such a site would establish. Banks and credit reporting agencies might be much more concerned, about where they sell and/or transmit identity information. Doctor's offices and other businesses might be much more careful about what information they gather and/or store, and who would have access to that information and for what purposes. And if the information isn't adequately protected, at least the victims will receive something for the injuries they suffer. At least there will be some protection for the individual victims.

References

Andrews v. TransUnion Corp., 7 F. Supp.2d 1056 (C.D. Calif. 1998), aff'd in part rev'd in part, 225 F.3d 1063 (9th Cir. 2000), cert. grtd., 532 U.S. 902 (2001).

California Penal Code, 528, et seq.

Caniglia, J. (2001). Prof Accused of Grabbing Tons of Loot in ID Scam. *Cleveland Plain Dealer*. Feb. 23, 2001 at 10A.

Fair Credit Billing Act, 15 U.S.C. §1681.

Foley, L. (2000). Prepared statement: Testimony for the California Legislative Service Comm. On Transportation: Special Oversight Hearing on Identity Theft. *California Dept. of Motor Vehicles* (available at http://www.privacyrights.org/ar/DMV-idtheft.htm).

Guzman v. Toyota Motor Credit Corp., 745 So.2d 1123 (Fla. App. 1999).

Identity Thief Uses Public Information to Establish Credit Accounts. *Consumer Financial Services Law Report.* June 26, 2000, LRP Publications.

Identity Theft and Assumption Deterrence Act, 1998, Pub. Law 105-318, 112 Stat. 3007, 18 U.S.C.§1028 (1998).

Idaho Code §28-51-101.

Ivey, R. W. (2000). Prepared statement: Protecting Privacy and Preventing Misuse of the Social Security Number. *Hearings on H.R. 4857 Before the Subcomm. On Social Security of the House Ways and Means Comm.*, 106th Congress.

King, T. (1999). Stolen Identities; Indianapolis Attorney Recovering from Identity Theft. *The Indiana Lawyer*, March 3, 1999.

Mattly v. Spiegel, Inc., 19 S.W.3d 890 (Tex. App., 2000).

Ohio Rev. Code §2913.49.

Patrick v. Union State Bank, 681 So.2d 1364 (Ala. 1996).

Polzer v. TRW, Inc., 682 N.Y.S.2d 194 (1998).

Restatement (Second) of Torts §442. ALI-ABA.

Stanley, J. (2001). Review of Selected 2000 California Legislation: Supporting Victims in Recovering From the Crime of the Information Age. *McGeorge Law Review.*McGeorge School of Law, University of the Pacific. Winter, 2001.

Truth-in-Lending Act, 15 U.S.C. §1643.

TRW, Inc. v. Andrews, ___ U.S. ___, 2001. U.S. Lexis 10306 (2001).

U.S. Federal Trade Commission (2001). *Identity Theft Complaint Data. Figures and Trends on Identity Theft, November 1999 to June 2001.*

U.S. General Accounting Office (1998). *Identity Fraud. Information on Prevalence Cost and Internet Impact is Limited*.