SEAN B. HOAR*

Current Developments

Identity Theft: The Crime of the New Millennium

I

The Nature of the Problem

Identity theft has been referred to by some as the crime of the new millennium.[1] It can be accomplished anonymously, easily, through a variety of means, and the consequences to the victim can be devastating. Identity theft is simply the theft of identity information such as a name, date of birth, Social Security number (SSN), or a credit card number. The mundane activities of a typical consumer during the course of a regular day may provide tremendous opportunities for an identity thief: purchasing gasoline, meals, clothes, or tickets to an athletic event; renting a car, a video, or home-improvement tools; purchasing gifts or trading stock on-line; receiving mail; or taking out the garbage or recycling. Any activity in which identity information is shared or made available to others creates an opportunity for identity theft.

It is estimated that identity theft has become the fastest growing financial crime in America, and perhaps, the fastest growing crime of any kind in our society.[2] According to the Federal Trade Commission (FTC), it received the highest number of consumer fraud complaints in 2001. Identity theft accounted for forty-two percent of the 204,000 complaints entered into the

* Assistant United States Attorney, District of Oregon.

[1] *Identity Thieves*, Reg. Guard (Eugene, Or.), Apr. 30, 2000, at 1A.

[2] *See Identity Theft: Is There Another You?: Joint Hearing Before the House Subcomms. on Telecommunications, Trade and Consumer Protection, and on Finance and Hazardous Materials, of the House Comm. on Commerce*, 106th Cong. 16 (1999) (statement of Rep. John B. Shadegg).

FTC's Consumer Sentinel database last year.[3] It is believed that terrorists have long utilized identity theft to obtain employment and access to secure locations, such as airports. Terrorists have also used these and similar means to obtain driver's licenses, hazardous material licenses, and bank and credit accounts through which terrorism-financing dollars are transferred.[4]

The illegal use of identity information has increased exponentially in recent years. In fiscal year 1999 alone, the Social Security Administration (SSA) Office of Inspector General (OIG) Fraud Hotline[5] received approximately 62,000 allegations involving SSN misuse. The widespread use of SSNs as identifiers has reduced their security and has increased their likelihood of being objects of identity theft. The expansion and popularity of conducting commercial transactions via the Internet has increased the opportunities to commit crimes involving identity theft. Further, the continued trend of posting official information over the Internet for the benefit of citizens and customers alike has also increased opportunities to obtain private information for illegal purposes.[6]

On May 31, 1998, in support of the Identity Theft and Assumption Deterrence Act of 1998,[7] the General Accounting Office (GAO) released a briefing report on issues relating to identity fraud entitled "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited."[8] The report found that methods used to obtain identity information ranged from basic street theft

[3] Press Release, Federal Trade Commission, Identity Theft Heads the FTC's Top 10 Consumer Fraud Complaints of 2001 (Jan. 23, 2002), *available at* http://www.ftc.gov/opa/2002/01/idtheft.htm.

[4] *The Financial War on Terrorism and the Administration's Implementation of the Anti-Money Laundering Provisions of the USA Patriot Act: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 107th Cong. (2002) (statement of Michael Chertoff, Assistant Attorney General, Criminal Division).

[5] The SSA OIG Fraud Hotline is 800-269-0271, and correspondence can be directed to P.O. Box 17768, Baltimore, MD 21235, to its Web site at http://www.ssa.gov, via e-mail to oig.hotline@ssa.gov, or by fax at 410-597-0118. *See* Office of the Inspector Gen., Soc. Sec. Admin., SSA Fraud Hotline, *available at* http://www.ssa.gov/ oig/guideline.htm.

[6] Public Workshop: Identity Theft Prevention, 65 Fed. Reg. 51,049 (Aug. 22, 2000).

[7] The Identity Theft and Assumption Deterrence Act was enacted on October 30, 1998. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-38, 112 Stat. 3007.

[8] U.S. Gen. Accounting Office, Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited, Briefing Report No. GAO/GGD-98-100BR (May 1, 1998).

to sophisticated, organized crime schemes involving the use of computerized databases or the bribing of employees with access to personal information on customer or personnel records.[9] The report also found the following: In 1995, ninety-three percent of arrests made by the U.S. Secret Service Financial Crimes Division involved identity theft. In 1996 and 1997, ninety-four percent of financial crimes arrests involved identity theft. The Secret Service stated that actual losses to individuals and financial institutions which the Secret Service had tracked involving identity fraud totaled $442 million in fiscal year 1995, $450 million in fiscal year 1996, and $745 million in fiscal year 1997.[10] The SSA OIG stated that SSN misuse in connection with program fraud increased from 305 in fiscal year 1996 to 1,153 in fiscal year 1997.[11] Postal inspection investigations showed that identity fraud was perpetrated by organized crime syndicates, especially to support drug trafficking, and had a nationwide scope.[12] Trans Union Corporation, one of the three major national credit bureaus, stated that two-thirds of its consumer inquiries to its fraud victim department involved identity fraud. Such inquiries had increased from an average of less than three thousand a month in 1992 to over forty-three thousand a month in 1997.[13] VISA U.S.A., Inc., and MasterCard International, Inc., both stated that overall fraud losses from their member banks were in the hundreds of millions of dollars annually.[14] MasterCard stated that dollar losses relating to identity fraud represented about ninety-six percent of its member banks' overall fraud losses of $407 million in 1997.[15]

Victims of identity theft often do not realize they have become victims until they attempt to obtain financing on a home or a vehicle. Only then, when the lender tells them that their credit history makes them ineligible for a loan, do they realize something is terribly wrong. When they review their credit report, they first become aware of credit cards for which they have never applied, bills long overdue, unfamiliar billing addresses, and inquiries from unfamiliar creditors. Even if they are able to iden-

[9] *Id*. at 1.
[10] *Id*. at 29.
[11] *Id*. at 31.
[12] *Id*. at 35.
[13] *Id*. at 41.
[14] *Id*. at 42-45.
[15] *Id*. at 45.

tify the culprit, it may take months or years, tremendous emotional anguish, many lost financial opportunities, and large legal fees, to clear up their credit history.

II

How Does Identity Theft Occur?

Identity theft occurs in many ways, ranging from careless sharing of personal information, to intentional theft of purses, wallets, mail, or digital information. In public places, for example, thieves engage in "shoulder surfing"—watching you from a nearby location as you enter your telephone calling card number or credit card number—or listen in on conversations while you give your credit card number over the telephone. Inside your home, thieves may obtain information from your personal computer while you are on-line and while they anonymously sit in the comfort of their own home. When you are away from your home or your car, identity thieves may burglarize your home or break into your car for identity information. Outside your home, thieves steal your mail, garbage or recycling material. Outside medical facilities or businesses, thieves engage in "dumpster diving"—going through garbage cans, large dumpsters or recycling bins—to obtain identity information which includes credit or debit card receipts, bank statements, medical records such as prescription labels, or other records that bear your name, address, or telephone number. Identity thieves might engage in "skimming"—they might use an electronic device to download information from your credit/debit card accounts. Identity thieves might also engage in "pretexting"—they might contact a credit bureau or a financial institution and falsely claim to be you or another person who might have a lawful right to access your identity information. Once the identity thief obtains your identity information, they might visit a number of credit card sites on the Internet and begin to destroy your credit history.

Identity theft can be accomplished through simple, low tech methods such as the theft of pre-approved credit solicitations, new checks from a mailbox, or the theft of a garbage can or recycling bin left at curbside. Identity theft can also be accomplished through complex, high-tech methods, such as the execution of software programs that mirror keystrokes on a computer or Web site. Regardless of how the crime is accomplished, however, it can be economically devastating to its victims.

In a recent Oregon case, a ring of thieves obtained identity information by stealing mail, garbage, and recycling material by breaking into cars and by hacking into Web sites and personal computers. The thieves traded the stolen information for methamphetamine, cellular telephones, or other favors. Before they were arrested, they had gained access to an estimated four hundred credit card accounts and had made an estimated $400,000 in purchases on those fraudulently obtained accounts. One aspect of the case involved the theft of pre-approved credit card solicitations, activating the cards, and having them sent to drop boxes or third-party addresses. Another scam involved taking names, dates of birth, and SSNs from discarded medical, insurance, or tax information and obtaining credit cards at various sites on the Internet. The thieves found most credit card companies to be unwitting allies. One of the thieves boasted about successfully persuading a bank to grant a higher credit limit on a fraudulently obtained credit card account. Another aspect of the case involved the use of a software application to hack into commercial Web sites or personal computers and mirror keystrokes to capture credit card account information.[16] Two of the offenders were prosecuted federally for conspiracy to commit computer fraud and mail theft under 18 U.S.C. §§ 1030(a)(4), 371, and 1708, and consented to the forfeiture of computer equipment obtained as a result of the fraudulent activity pursuant to 18 U.S.C. § 982(a)(2)(B).[17] One defendant was sentenced to serve a forty-one month term of imprisonment and required to pay $70,025.98 in restitution.[18] The other defendant was sentenced to serve a fifteen month term of imprisonment and required to pay $52,379.03 in restitution.[19]

III

How Can Identity Theft Be Investigated and Prosecuted?

The investigation of identity theft is challenging. It is labor intensive and individual cases are usually too small to be considered for federal prosecution. Furthermore, victims often do not

[16] *Identity Thieves*, *supra* note 1, at 1A.

[17] United States v. Massey, No. 99-60116-01-AA (D. Or. Oct. 6, 2000); United States v. Melton, No. 99-60118-01-AA (D. Or. July 19, 2000).

[18] United States v. Massey, No. 99-60116-01-AA (D. Or. Oct. 6, 2000).

[19] United States v. Melton, No. 99-60118-01-AA (D. Or. July 19, 2000).

realize they have been victimized until weeks or months after the crime has been committed and can provide little assistance to law enforcement. In short, identity theft has become the fastest-growing financial crime in the United States and perhaps the fastest-growing crime of any kind in our society because offenders are seldom held accountable. Consequently, it has become a priority for the Departments of Justice and Treasury and the FTC to pursue effective means of prevention, investigation, and prosecution of identity theft offenses. Toward that end, workshops have been held for the purpose of identifying the best practices to combat identity theft, including remediation, prevention, and law enforcement strategies. Workshop participants have included prevention specialists, federal agency representatives, and state and federal investigators and prosecutors.[20]

The experience of workshop participants is that law enforcement agencies at all levels, federal and non-federal, must work together in investigating identity theft. Multi-agency task forces have proven successful in investigating and prosecuting identity theft. By utilizing task forces, member agencies can pool scarce resources to investigate and prosecute identity theft offenses and provide prevention training. Multi-agency task forces are also better equipped to pursue thieves who steal identity information from multiple victims in multiple jurisdictions. By working closely with state and federal prosecutors, multi-agency task forces are also more likely to successfully hold such thieves accountable for their crimes. Outreach to private industry is necessary as a prevention strategy, and it facilitates the identification of offenders.

Identity theft cases involving large numbers of victims present unique challenges. Victims include both the individual persons who suffer the theft of their identity information and the financial institutions that suffer monetary losses. One challenge is communication with victims. Communication is necessary to obtain fundamental investigative information, including loss and

[20] The author served as a panelist in one such workshop in Alexandria, Virginia in December 2000, which was sponsored by the Department of Treasury through the Secret Service, the Department of Justice through its Fraud Section, and the FTC. It was the culmination of a series of events highlighting the problem of identity theft and pursuing effective means of prevention, investigation, and prosecution. The workshop included information about how to prevent identity theft, and it utilized panel discussions with investigators and prosecutors to identify effective ways to investigate and prosecute identity theft cases.

restitution information. In complex cases, it is imperative to devise a system for communication with victims as soon as possible in the investigative phase of a case. Most prosecutors' offices have a victim/witness unit which is established to work closely with and provide essential services to crime victims. In establishing systems to communicate with identity theft victims, investigators and prosecutors should work with the victim/witness unit to identify the best communication system for the case.

A. Federal Criminal Laws

There are a number of federal laws applicable to identity theft, some of which may be used for prosecution of identity theft offenses, and some which exist to assist victims in repairing their credit history. The primary identity theft statute is 18 U.S.C. § 1028(a)(7). It was enacted on October 30, 1998, as part of the Identity Theft and Assumption Deterrence Act (Identity Theft Act).[21] The Identity Theft Act was needed because 18 U.S.C. § 1028 previously addressed only the fraudulent creation, use, or transfer of identification *documents*, and not the theft or criminal use of the underlying personal *information*. The Identity Theft Act added § 1028(a)(7), which criminalizes fraud in connection with the unlawful theft and misuse of personal identifying information, regardless of whether the information appears or is used in documents.[22] Section 1028(a)(7) provides that it is unlawful for 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."[23]

The Identity Theft Act amended the penalty provisions of § 1028(b) by extending its coverage to offenses under the new § 1028(a)(7) and applying more stringent penalties for identity thefts involving property of value.[24] Section 1028(b)(1)(D) provides for a term of imprisonment of not more than fifteen years when an individual commits an offense that involves the transfer or use of one or more means of identification if, as a result of the offense, anything of value aggregating one thousand dollars or

[21] *See supra* note 7.
[22] 18 U.S.C. § 1028(a)(7) (Supp. IV 1998).
[23] *Id.*
[24] *Id.* § 1028(b).

more during any one-year period is obtained.[25] Otherwise, § 1028(b)(2)(B) provides for imprisonment of not more than three years.[26] The Identity Theft Act added § 1028(f), which provides that attempts or conspiracies to violate § 1028 are subject to the same penalties as those prescribed for substantive offenses under § 1028.[27]

The Identity Theft Act amended § 1028(b)(3) to provide that if the offense is committed to facilitate a drug trafficking crime, or in connection with a crime of violence, or is committed by a person previously convicted of identity theft, the individual is subject to a term of imprisonment of not more than twenty years.[28] If the offense is committed to facilitate an act of international terrorism, the individual is subject to a term of imprisonment of not more than twenty-five years.[29] The Identity Theft Act also added § 1028(b)(5) which provides for the forfeiture of any personal property used or intended to be used to commit the offense.[30]

Section 1028(d)(4) defines "means of identification," as used in § 1028(a)(7), to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[31] It covers several specific examples, such as: name, social security number, date of birth, government-issued driver's license, and other numbers; unique biometric data, such as fingerprints, voice print, retina or iris image, or other physical representation; unique electronic identification number; and telecommunication identifying information or access device.[32]

Section 1028(d)(1) modifies the definition of "document-making implement" to include computers and software specifically configured or primarily used for making identity documents.[33] The Identity Theft Act is intended to cover a variety of individual identification information that may be developed in the future and utilized to commit identity theft crimes.

---

[25] *Id.* § 1028(b)(1)(D).
[26] *Id.* § 1028(b)(2)(B).
[27] *Id.* § 1028(f).
[28] *Id.* § 1028(b)(3).
[29] *Id.* § 1028(b)(4).
[30] *Id.* § 1028(b)(5).
[31] *Id.* § 1028(d)(4).
[32] *Id.* § 1028(d)(4)(A)-(D).
[33] *Id.* § 1028(d)(1).

The Identity Theft Act also directed the United States Sentencing Commission to review and amend the United States Sentencing Guidelines to provide appropriate penalties for each offense under § 1028.[34] The Sentencing Commission responded to this directive by adding section 2B1.1(b)(9), which provides the following:

> (9) If the offense involved—
> (A) the possession or use of any device-making equipment;
> (B) the production or trafficking of any unauthorized access device or counterfeit access device; or
> (C) (i) the unauthorized transfer or use of any means of identification unlawfully to produce or obtain any other means of identification; or (ii) the possession of five or more means of identification that unlawfully were produced from another means of identification or obtained by the use of another means of identification, increase by 2 levels. If the resulting offense level is less than level 12, increase to level 12.[35]

For most fraud offenses, the loss would have to be more than thirty thousand dollars for the resulting offense level to be level 12.[36] This minimum offense level accounts for the fact that the means of identification that were "bred" (i.e., produced or obtained) often are within the defendant's exclusive control, making it difficult for the individual victim to detect that the victim's identity has been "stolen." Generally, the victim does not become aware of the offense until certain harms have already occurred (e.g., a damaged credit rating or an inability to obtain a loan). The minimum offense level also accounts for the nonmonetary harm associated with these types of offenses, much of which may be difficult or impossible to quantify (e.g., harm to the individual's reputation or credit rating, inconvenience, and other difficulties resulting from the offense). The legislative history of the Identity Theft Act indicates that Congress was especially concerned with providing increased punishment for this type of harm.[37]

In providing for an offense level of 12 for certain types of iden-

---

[34] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 4, 112 Stat. 3007, 3009-10.

[35] U.S. SENTENCING GUIDELINES MANUAL § 2B.1.1(b)(9) (2001).

[36] Section 2B1.1(a) provides for a base offense level of 6 for most fraud offenses. *Id.* § 2B.1.1(a). Section 2B1.1(b)(1)(D) provides that if the loss exceeded $30,000, the offense level is to be increased by six levels, which results in a level 12 offense level. *Id.* § 2B1.1(b)(1)(D).

[37] *See id.* § 2B1.1, cmt. background.

tity theft, the Sentencing Commission acknowledged that the economic harm from identity theft is difficult to quantify, and that whatever the identifiable loss, offenders should be held accountable. Identity thieves will merit an additional two level increase if the offense involves more than ten, but less than fifty, victims.[38] If the offense involves fifty or more victims, it will merit an additional four level increase.[39] Identity thieves who play a managerial role in the offense may also receive an additional two- to four-level upward adjustment when multiple defendants are involved.[40]

The Identity Theft Act also directed the FTC to establish a procedure to log in and acknowledge receipt of complaints from victims of identity theft, to provide educational materials to these victims and refer the complaints to appropriate entities.[41] The FTC has responded to this directive by developing a tremendously helpful Web site, great educational materials, a hotline for complaints, and a central database for information. The FTC has become a primary referral point for victims of identity theft and a tremendous resource for these victims and law enforcement.[42]

B. Other Federal Offenses

Identity theft is often committed to facilitate other crimes, although it is frequently the primary goal of the offender. Schemes to commit identity theft may involve a number of other statutes including identification fraud,[43] credit card fraud,[44] computer fraud,[45] mail fraud,[46] wire fraud,[47] financial institution fraud,[48]

---

[38] *Id.* § 2B1.1(b)(2)(A)(i).

[39] *Id.* § 2B1.1(b)(2)(B).

[40] *Id.* § 3B1.1.

[41] Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 5, 112 Stat. 3007, 3010.

[42] The FTC Identity Theft Clearinghouse is located at 600 Pennsylvania Avenue, N.W., Washington, DC 20580, its Web site can be found at http://www.consumer.gov/idtheft, and the FTC Identity Theft Hotline is 877-IDTHEFT (438-4338), and TDD is 866-653-4261. *See* Fed. Trade Comm'n, Identity Crisis . . . What to Do if Your Identity Is Stolen (Feb. 2000), *available at* http://www.ftc.gov/bcp/conline/pubs/general/idtheftfact.htm.

[43] 18 U.S.C. § 1028(a)(1)-(6) (1994 & Supp. IV 1998).

[44] *Id.* § 1029.

[45] *Id.* § 1030.

[46] *Id.* § 1341.

[47] *Id.* § 1343.

[48] *Id.* § 1344.

mail theft,[49] immigration document fraud,[50] and narcotics trafficking.[51] For example, computer fraud may be facilitated by the theft of identity information when stolen identity information is used to fraudulently obtain credit on the Internet. Computer fraud may also be the primary vehicle to obtain identity information when the offender obtains unauthorized access to another computer or Web site to obtain such information. These acts might result in the offender being charged with both identity theft under 18 U.S.C. § 1028(a)(7) and computer fraud under 18 U.S.C. § 1030(a)(4). Regarding computer fraud, note that section 2B1.1(d) of the United States Sentencing Guidelines provides for a minimum guideline sentence, notwithstanding any other adjustment, of a six-month term of imprisonment if a defendant is convicted of computer fraud under 18 U.S.C. § 1030(a)(4) or (5).[52]

C. Recent Federal Cases

A number of cases have recently been prosecuted under 18 U.S.C. § 1028(a)(7), including the following. In the Central District of California, a man was sentenced to a twenty-seven month term of imprisonment for obtaining private bank account information about an insurance company's policyholders, while serving as a temporary employee of the company. Thereafter he used that information to deposit over $764,000 in counterfeit bank drafts and withdraw funds from accounts of policyholders.[53] In the District of Delaware, one defendant was sentenced to a thirty-three month term of imprisonment and $160,910.87 in restitution, and another defendant to a forty-one month term of imprisonment and $126,298.79 in restitution for obtaining names and SSNs of high-ranking military officers from an Internet Web site and using them to apply on-line for credit cards and bank and corporate credit in the officers' names.[54]

In the District of Oregon, seven defendants were sentenced to imprisonment for their roles in a heroin/methamphetamine trafficking organization, which included entering the United States illegally from Mexico and obtaining SSNs of other persons. The

[49] *Id.* § 1708.
[50] *Id.* § 1546.
[51] 21 U.S.C. § 841(a)(1) (1994).
[52] U.S. SENTENCING GUIDELINES MANUAL § 2B1.1(d)(1) (2001).
[53] United States v. Johnson, No. 99-926 (C.D. Cal. Jan. 31, 2000).
[54] United States v. Christian, No. 00-3-1 (D. Del. Aug. 9, 2000).

SSNs were then used to obtain temporary employment and identification documents in order to facilitate the distribution of heroin and methamphetamine. In obtaining employment, the defendants used false alien registration receipt cards, in addition to the fraudulently obtained SSNs, which provided employers enough documentation to complete employment verification forms.[55] Some of the defendants also used the fraudulently obtained SSNs to obtain earned income credits on tax returns fraudulently filed with the Internal Revenue Service (IRS).[56] Some relatives of narcotics traffickers were arrested in possession of false documents and were charged with possessing false alien registration receipt cards and with using the fraudulently obtained SSNs to obtain employment.[57] A total of thirty-one defendants have been convicted in the case to date, sixteen federally and fifteen at the state level.[58]

---

[55] United States v. Cortes, No. 00-60045-01-HO (D. Or. Nov. 14, 2001); United States v. Gomez, No. 00-60034-01-HO (D. Or. Feb. 28, 2001); United States v. Salgado, No. 00-60039-01-HO (D. Or. Jan. 18, 2001); United States v. Sanchez, No. 00-60040-01-HO (D. Or. Nov. 21, 2000); United States v. Rios, No. 00-60035-01-HO (D. Or. Nov. 7, 2000); United States v. Sanchez, No. 00-60080-01-HO (D. Or. Aug. 31, 2000); United States v. Diaz, No. 00-60038-01-HO (D. Or. Aug. 10, 2000).

[56] United States v. Sanchez, No. 00-60040-01-HO (D. Or. Nov. 21, 2000).

[57] United States v. Diaz, No. 00-60138-01-AA (D. Or. Sept. 21, 2000); United States v. Calderon, No. 00-60046-01-HO (D. Or. May 10, 2000); United States v. Delgadillo, No. 00-60058-01-HO (D. Or. Apr. 20, 2000); United States v. Salgado, No. 00-60061-01-HO (D. Or. Apr. 20, 2000); United States v. Tellez, No. 00-60060-01-HO (D. Or. Apr. 20, 2000).

[58] United States v. Cortez, No. 00-60045-01-HO (D. Or. Nov. 16, 2001); United States v. Guerero, No. 00-60037-01-HO (D. Or. Apr. 27, 2001); United States v. Gomez, No. 00-60034-01-HO (D. Or. Feb. 28, 2001); United States v. Carrillo, No. 00-60036-01-HO (D. Or. Feb. 11, 2001); United States v. Avila, No. 00-60044-01-HO (D. Or. Feb. 2, 2001); United States v. Salgado, No. 00-60039-01-HO (D. Or. Jan. 18, 2001); United States v. Sanchez, No. 00-60131-01-HO (D. Or. Jan. 9, 2001); United States v. Talbot, No. 00-60081-01-HO (D. Or. Dec. 31, 2000); United States v. Sanchez, No. 00-60143-01-HO (D. Or. Dec. 13, 2000); United States v. Sanchez, No. 00-60040-01-HO (D. Or. Nov. 21, 2000); United States v. Rios, No. 00-60035-01-HO (D. Or. Nov. 7, 2000); United States v. Sanchez, No. 00-60080-01-HO (D. Or. Aug. 31, 2000); United States v. Ramirez, No. 00-60043-01-HO (D. Or. Aug. 30, 2000); United States v. Diaz, No. 00-60038-01-HO (D. Or. Aug. 10, 2000); United States v. Lopez, No. 00-60038-01-HO (D. Or. Aug. 10, 2000); United States v. Calderon, No. 00-60046-01-HO (D. Or. May 10, 2000); State v. Gasso, No. 005682FE (Cir. Ct. Jackson County, Or., Oct. 26, 2001); State v. Jacobs, No. 0100508FE (Cir. Ct. Jackson County, Or., Feb. 7, 2001); State v. Kistle, No. 0005652FE (Cir. Ct. Jackson County, Or., Jan. 26, 2001); State v. Williams, No. 004533FE (Cir. Ct. Jackson County, Or., Jan. 12, 2001); State v. Byrne, No. 004363FE (Cir. Ct. Jackson County, Or., Jan. 9, 2001); State v. Davis, No. 006276FE (Cir. Ct. Jackson County, Or., Dec. 13, 2000); State v. Guiterrez, No. 005257FE (Cir. Ct. Jackson County, Or., Nov. 8, 2000); State v. Gilhousen, No. 002225FE (Cir. Ct. Jackson County, Or., Nov. 7, 2000); State v.

D. Fraudulent Access to Financial Information: The Gramm-Leach-Bliley Act

Given the tremendous increase in identity theft crime and gaps in accountability with commercial entities engaged in information sharing, in 1999 Congress passed The Fraudulent Access to Financial Information subchapter of the Gramm-Leach-Bliley Act (GLEBA).[59] It contains, among other things, specific prohibitions against obtaining financial institution customer information by means of false pretenses (pretext calling or "pretexting") and directs federal banking regulatory agencies to ensure that financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.[60] GLEBA is primarily directed at reducing opportunities for persons to impersonate victims of identity theft.

GLEBA prohibits the making of false, fictitious, or fraudulent statements to an officer, employee, or agent of a financial institution, or to a customer of a financial institution, in an effort to obtain or attempt to obtain "customer information of a financial institution relating to another person."[61] GLEBA also prohibits any person from obtaining such customer information by "providing any document to an officer, employee or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fic-

King, No. 003594FE (Cir. Ct. Jackson County, Or., Oct. 31, 2000); State v. Campbell, No. 002376FE (Cir. Ct. Jackson County, Or., Oct. 18, 2000); State v. Golden, No. 002726FE (Cir. Ct. Jackson County, Or., Oct. 18, 2000); State v. Ponce, No. 004317MI (Cir. Ct. Jackson County, Or., Sept. 13, 2000); State v. Right, No. 002374FE (Cir. Ct. Jackson County, Or., Sept. 7, 2000); State v. Eaton, No. 002378FE (Cir. Ct. Jackson County, Or., Aug. 25, 2000); State v. Kelley, No. 002377FE (Cir. Ct. Jackson County, Or., July 24, 2000).

[59] Gramm-Leach-Bliley Act (GLEBA) §§ 521-527, 15 U.S.C.A. §§ 6821-6827 (West Supp. 2001).

[60] *See id.*

[61] 15 U.S.C.A. § 6821(a)(1)-(2). Financial institutions are defined as "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution." *Id.* § 6827(4)(A). Certain financial institutions, such as brokerage firms, insurance companies, credit card issuers, etc., are specifically included in the definition. *Id.* § 6827(4)(B). "Customer information of a financial institution" is defined as "any information maintained by or for a financial institution which is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer." *Id.* § 6827(2).

titious, or fraudulent statement or representation."[62] GLEBA also prohibits anyone from requesting a person "to obtain customer information of a financial institution, knowing that the person will obtain, or attempt to obtain, the information from the institution in any manner" prohibited under GLEBA.[63]

Violators of GLEBA are subject to a criminal penalty of imprisonment of not more than five years and a fine of not more than $250,000 for individuals or $500,000 for organizations if they knowingly and intentionally violate, or knowingly and intentionally attempt to violate, GLEBA.[64] If a person violates GLEBA while violating another United States law, or as a part of a pattern of criminal activity involving more than $100,000 in a twelve-month period, he is subject to an enhanced fine of $500,000 for individuals or $1,000,000 for organizations and imprisonment for not more than ten years or both.[65]

GLEBA requires federal banking agencies, the Securities and Exchange Commission (SEC), and self-regulatory organizations to review regulations and guidelines applicable to financial institutions under their jurisdiction and prescribe such revisions as may be necessary to ensure that these institutions have in place requisite policies, procedures, and controls to prevent the unauthorized disclosure of customer financial information and deter and detect activities prohibited by GLEBA.[66] Administrative enforcement by the FTC and other regulatory agencies is also provided by GLEBA.[67]

E. Federal Credit Laws

It is important for consumers to have at least a cursory understanding of credit laws that impact identity theft. It is also important for those who assist identity theft victims to understand pertinent credit laws. Such an understanding can help repair a damaged credit history. The Fair Credit Reporting Act establishes procedures and timeframes for correcting mistakes on credit records and requires that your record only be provided for legitimate business, credit, or employment needs.[68] The Truth in

[62] *Id.* § 6821(a)(3).
[63] *Id.* § 6821(b).
[64] *Id.* § 6823(a); 18 U.S.C. § 3571(b)(3), (c)(3) (1994).
[65] 15 U.S.C.A. § 6823(b); 18 U.S.C. § 3571(b)(3), (c)(3).
[66] 15 U.S.C.A. § 6825.
[67] *Id.* § 6822.
[68] 15 U.S.C. §§ 1681-1681t (1994 & Supp. IV 1998).

Lending Act limits liability for unauthorized credit card charges in most cases to fifty dollars.[69] The Fair Credit Billing Act establishes procedures for resolving billing errors on credit card accounts *if* the unauthorized charge is reported within certain timeframes.[70] The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection.[71] The Electronic Fund Transfer Act provides consumer protections for transactions using a debit card or electronic means to debit or credit an account.[72] It also limits a consumer's liability for unauthorized electronic fund transfers *if* the unauthorized transfer is reported within certain time frames. If an ATM or debit card is reported lost or stolen within two business days of the loss or theft, the losses are limited to fifty dollars. If reported after two business days but within sixty days of the first statement showing an unauthorized transfer, the losses are limited to five hundred dollars. Otherwise, losses may only be limited by the amount obtained.[73]

F. State Criminal Laws

Most states have laws prohibiting the theft of identity information.[74] Where specific identity theft laws do not exist, the prac-

---

[69] *Id.* § 1643(a)(1)(B).

[70] *Id.* § 1666. Generally, billing errors must be reported to a creditor within sixty days after the first bill containing the error was mailed to the consumer. *See id.* § 1666(a).

[71] *See id.* §§ 1692e-1692f.

[72] *See id.* §§ 1693-1693r.

[73] *Id.* § 1693g(a).

[74] ALASKA STAT. § 11.46.180 (Michie 2000); ARIZ. REV. STAT. ANN. § 13-2008 (West Supp. 2001); ARK. CODE ANN. § 5-37-227 (Michie Supp. 2001); CAL. PENAL CODE §§ 530.5-.7 (West Supp. 2002); COLO. REV. STAT. § 18-5-102 (2001); CONN. GEN. STAT. ANN. § 53a-129a (West 2001); FLA. STAT. ANN. § 817.568 (West Supp. 2002); GA. CODE ANN. §§ 16-9-121, 16-9-127 (Harrison 1998); IDAHO CODE § 18-3126 (Michie Supp. 2001); 720 ILL. COMP. STAT. 5/16G-1 to 5/16G-25 (West Supp. 2002); IND. CODE ANN. § 35-43-5-4 (Michie Supp. 2001); IOWA CODE ANN. § 715A.8 (West Supp. 2002); KAN. STAT. ANN. § 21-4018 (Supp. 2001); KY. REV. STAT. ANN. § 514.160 (Michie Supp. 2001); LA. REV. STAT. ANN. § 14:67.16 (West Supp. 2002); ME. REV. STAT. ANN. tit. 17-A, § 354(2)(A) (West Supp. 2002); MD. ANN. CODE art. 27, § 231 (Supp. 2001); MASS. ANN. Laws ch. 266, § 37E (Law. Co-op. Supp. 2002); MICH. COMP. LAWS ANN. § 750.285 (West Supp. 2002); MINN. STAT. ANN. § 609.527 (West Supp. 2002); MISS. CODE ANN. § 97-19-85 (West 1995); MO. ANN. STAT. § 570.223 (West Supp. 2002); NEV. REV. STAT. §§ 205.463-.465 (Michie 2001 & Supp. 2001); N.H. REV. STAT. ANN. § 638:26 (Supp. 2001); N.J. STAT. ANN. § 2C:21-17 (West Supp. 2002); N.C. GEN. STAT. § 14-113.20 (1999); N.D. CENT. CODE § 12.1-23-11 (Supp. 2001); OHIO REV. CODE ANN. § 2913.49 (Anderson 1999); OKLA. STAT.

tices may be prohibited under other state laws or the states may be considering such legislation. Guam and the U.S. Virgin Islands also have laws prohibiting the theft of identity information.[75]

IV

How Can Identity Theft Be Prevented?[76]

While it is extremely difficult to prevent identity theft, the best approach is to be proactive and take steps to avoid becoming a victim.

A. Only Share Identity Information When Necessary

Be cautious about sharing personal information with anyone who does not have a legitimate need for the information. For instance, credit card numbers should never be provided to anyone over the telephone unless the consumer has initiated the call and is familiar with the entity with whom they are doing business. Likewise, SSNs should not be provided to anyone other than employers or financial institutions who need the SSN for wage, interest, and tax reporting purposes. Businesses may legitimately inquire about an SSN if conducting a credit check for purposes of financing a purchase. Some entities, however, may simply want the SSN for recordkeeping purposes. Businesses may choose not to provide a service or benefit without obtaining a person's SSN, but the choice as to whom an SSN is provided should be exer-

Ann. tit. 21, § 1533.1 (West Supp. 2002); Or. Rev. Stat. § 165.800 (2001); 18 Pa. Stat. Ann. tit. 18, § 4120 (West Supp. 2002); R.I. Gen. Laws §§ 11-49.1-1 to 11-49.1-4 (2001); S.C. Code Ann. § 16-13-510 (Law. Co-op. Supp. 2001); S.D. Codified Laws § 22-30A-3.1 (Michie Supp. 2001); Tenn. Code Ann. § 39-14-150 (Supp. 2001); Tex. Penal Code Ann. § 32.51 (Vernon Supp. 2001); Utah Code Ann. § 76-6-1102 (Supp. 2001); Va. Code Ann. § 18.2-186.3 (Michie Supp. 2001); Wash. Rev. Code Ann. § 9.35.020 (West Supp. 2002); W. Va. Code § 61-3-54 (Michie 2000); Wis. Stat. Ann. § 943.201 (West Supp. 2001); Wyo. Stat. Ann. § 6-3-901 (Michie 2001).

[75] 9 Guam Code Ann. § 46.80 (2001); 14 V.I. Code Ann. § 3003 (2001).

[76] A thorough guide to preventing and responding to identity theft can be found in Mari Frank & Beth Givens, Privacy Piracy! A Guide to Protecting Yourself from Identity Theft (1999). Related information can be found at http://www.identitytheft.org (last visited Mar. 29, 2002). The Federal Trade Commission (FTC) has also published a helpful guide regarding identity theft. Fed. Trade Comm'n, ID Theft: When Bad Things Happen to Your Good Name (2000), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. Related information can also be found at http://www.consumer.gov/idtheft. Also, the United States Postal Inspection Service has produced an excellent video about identity theft entitled *IDENTITY THEFT: The Game of the Name*.

cised with caution. In the event an entity, such as a hospital or a department of motor vehicles (DMV), assigns an SSN as a patient or client identification number, the customer should request that an alternative number be assigned.

B. When in Public, Exercise Caution When Providing Identity Information

"Shoulder surfers" regularly glean such information for their fraudulent use. Be especially cautious when entering account information at an automatic teller machine (ATM), or when entering long-distance calling card information on a public telephone. Likewise, be cautious when orally providing this type of information on a public telephone. Also, do not put identity information, such as an address or license plate number, on a key ring or anything similar that can easily be observed or lost. Identity information on such objects simply provides thieves easier means of finding and accessing homes and cars.

C. Do Not Carry Unnecessary Identity Information in a Purse or Wallet

The primary means for thieves to obtain identity information is through the loss or theft of purses and wallets.[77] To reduce the risk that identification information might be misappropriated, only carry the identity information necessary for use during the course of daily activities such as a driver's license, one credit or debit card, an insurance card, and membership cards that are regularly required for use. There should be no need to carry a Social Security card or anything containing an SSN. Likewise, there should be no need to carry a birth certificate or a passport. These items should be kept under lock and key in a safe or a safe deposit box. Credit or debit cards that are not regularly used should also be removed from a purse or wallet. The fewer pieces of identification carried in a purse or wallet, the easier it is to identify an individual piece that may have been lost or stolen, and the easier the task of notifying creditors and replacing such information should a purse or wallet be lost or stolen.

[77] Of all identity theft complaints filed with the FTC between November of 1999 and October of 2000, the loss or theft of a purse or wallet was the method by which thieves obtained identity information in forty-seven percent of the cases. Fed. Trade Comm'n, Figures and Trends on Identity Theft: November 1999 Through September 2000 (Oct. 24, 2000), *available at* http://www.ftc.gov/bcp/workshops/idtheft/reporttext.htm.

D. Secure Your Mailbox

The second most successful means for thieves obtaining identity information is through stolen mail.[78] Many thieves follow letter carriers at a discreet distance and steal mail immediately after it has been delivered to a residential mailbox. To make it harder for the thieves to succeed, do not place outgoing mail in residential mailboxes. Doing so, especially raising a red flag on a mailbox to notify the postal carrier of outgoing mail, is simply an invitation to steal. Deposit outgoing mail in locked postal collection boxes or at a local post office. If you prefer to have mail delivered to your residential address, install a mailbox which is secured by lock and key. Promptly remove mail after it has been delivered to your mailbox.

E. Secure Information on Your Personal Computer

Similar to telephonic inquiries, credit card numbers should not be provided to anyone on the Internet unless the consumer has initiated the contact and is familiar with whom they are doing business. In addition to cautiously choosing with whom identity information is shared, computer users should install a firewall[79] on their personal computers to prevent unauthorized access to stored information. This is especially true for digital subscriber line (DSL), cable modem, or other "always-on" connections. There are a number of quality firewall software applications that can be downloaded as freeware from sites on the Internet.[80] Computer users should never open e-mail from unknown, unsolicited sources. Doing so can provide access to a computer by a damaging virus or an unauthorized information gathering program. Computer users should also remove their names from e-mail marketing lists. Doing so will reduce the risk that a damaging program will access the computer.

---

[78] Mail theft was the method by which thieves obtained identity information in twenty-three percent of the cases reported to the FTC between November 1999 and September 2000. *Id*.

[79] A personal firewall is designed to run on an individual personal computer and isolate it from the rest of the Internet, thereby preventing unauthorized access to the computer. The user sets the level of desired security, and the firewall inspects each packet of data to determine if it should be allowed to get to or from the individual machine, consistent with the level of security.

[80] To identify firewall applications, simply use the term "firewall" in an on-line search and look for articles or sources of information about firewall products.

F. Keep Financial and Medical Records in a Secure Location

Thieves may be more interested in identity information from which they can access credit, than in physical property. It is important, therefore, to keep all financial and medical records, and any other information containing identity information, in a secure location under lock and key.

G. Shred Non-Essential Material Containing Identity Information

All non-essential documentary material containing any type of identity information should be shredded prior to being placed in garbage or recycling. The term "non-essential" should be interpreted as anything that an individual or business is not required by law or policy to retain. For individuals this includes credit or debit card receipts, canceled bank checks and statements, outdated insurance or financial information, and junk mail, especially pre-approved credit applications and subscription solicitations. For businesses or medical facilities, this includes receipts of completed credit or debit card transactions, outdated client files, or prescription labels. The best shredding is done through a cross-cut shredder which cuts paper into small pieces, making it extremely difficult to reconstruct documents. Expired credit or debit cards should also be cut into several pieces before being discarded.

H. "Sanitize" the Contents of Garbage and Recycling

All non-essential documentary material containing any type of identity information should be shredded before being placed in garbage or recycling. While junk mail or old financial documents may appear to be innocuous, they can be a goldmine when obtained by an identity thief.

I. Ensure That Organizations Shred Identity Information

Many businesses, firms, and medical facilities are not sensitive to privacy issues arising from discarded material. Many of these entities regularly dispose of material containing customer identity information (i.e., customer orders, receipts, prescription labels, etc.) into garbage cans, dumpsters, or recycling bins without shredding the material. Tremendous damage can be done by these practices. Customers of businesses, clients of firms, and pa-

tients of medical facilities should insist that all data be shredded before being discarded and that all retained data be kept in secure storage.

J. Remove Your Name from Mailing Lists[81]

Removing a name from a mailing list reduces the number of commercial entities having access to the identity information. It also reduces the amount of junk mail, including pre-approved credit applications and subscription solicitations, thereby reducing the risk that the theft of such mail will compromise privacy. Many financial institutions, such as banks and credit card companies, and even governmental agencies, market identity information of customers unless a request is received, in writing, that such information not be shared. Customers of such businesses and agencies should submit such requests, notifying the entity in writing of their desire to opt out of any mailing lists and to not have identity information shared.

K. Carefully Review Financial Statements

Promptly review all bank and credit card statements for accuracy. Pay attention to billing cycles. A missing bill may mean a thief has taken over an account and changed the billing address to avoid detection. Report any irregularities to the bank or credit card company immediately.

L. Periodically Request Copies of Credit Reports

Credit reports are available for nine dollars from the three major credit bureaus.[82] Credit bureaus must provide a free copy of the report if it is inaccurate due to fraud and it is requested in writing. The reports should be reviewed carefully to make sure

[81] To opt out of the mailing lists of the three major credit bureaus (Equifax, Experian, and Trans Union), call 888-567-8688. To opt out of many national direct mail lists, write to the Direct Marketing Association, DMA Preference Service, P.O. Box 9008, Farmingdale, NY 11735-9008. To opt out of many national direct e-mail lists, visit http://www.e-mps.org. To opt out of many national telemarketer lists, send your name, address, and telephone number to the Direct Marketing Association, DMA Telephone Preference Service, P.O. Box 9014, Farmingdale, NY 11735-9014.

[82] To order a report from Equifax, visit http://www.equifax.com, call 800-685-1111, or write P.O. Box 740241, Atlanta, GA 30374-0241. To order a report from Experian, visit http://www.experian.com, call 888-EXPERIAN (397-3742), or write P.O. Box 949, Allen, TX 75013-0949. To order a report from Trans Union, visit http://www.tuc.com, call 800-916-8800, or write P.O. Box 1000, Chester, PA 19022.

no unauthorized accounts have been opened or unauthorized changes made to existing accounts.

V

What Steps Should Be Taken by a Victim of Identity Theft?

When someone realizes they have become a victim of identity theft, they should take the following steps while keeping a log of all conversations, including dates, names, and telephone numbers. The log should indicate any time spent and expenses incurred in the event restitution can be obtained in a civil or criminal judgment against the thief. All conversations should be confirmed in writing with the correspondence sent by certified mail, return receipt requested. All correspondence should be kept in a secure location, under lock and key.

First, the victim should contact the fraud departments at each of the three major credit bureaus (Equifax, Experian, and Trans Union), inform the representative of the identity theft, and request that a "fraud alert" be placed on their file, as well as a statement asking that creditors call the victim before opening any new accounts.[83] This can help prevent an identity thief from opening additional accounts in the victim's name. The victim should inquire about how long the fraud alert will remain on the file, and what, if anything, must be done to extend the alert if necessary. Copies of credit reports from the credit bureaus should also be ordered. Credit bureaus must provide a free copy of the report if it is inaccurate due to fraud and it is requested in writing. The reports should be reviewed carefully to make sure no additional accounts have been opened or unauthorized changes made to existing accounts. Also, if the reports indicate that any "inquiries" were made from companies that opened fraudulent accounts, a request should be made to remove the "inquiries" from the report. A request should also be made for the credit bureaus to notify those who have received a credit report in the last six months and alert them to the disputed and

[83] To report fraud to Equifax, visit http://www.equifax.com, call 800-525-6285, or write P.O. Box 740241, Atlanta, GA 30374-0241. To report fraud to Experian, visit http://www.experian.com, call 888-EXPERIAN (397-3742), or write P.O. Box 949, Allen, TX 75013-0949. To report fraud to Trans Union, visit http://www.tuc.com, call 800-680-7289, or write Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634.

erroneous information. The victim should request a new copy of the reports after a few months to verify that the requested changes have been made and to ensure no new fraudulent activity has occurred.

Second, the victim should contact the security or fraud departments for any creditors of accounts in which fraudulent activity occurred. The telephone numbers for these creditors can be obtained from the credit bureaus. Creditors can include businesses, credit card companies, telephone and other utility companies, banks, and other lenders. All conversations should be confirmed with written correspondence. It is particularly important to notify credit card companies in writing because it is required by the consumer protection laws set forth above.[84] The victim should immediately close accounts that have been tampered with and open new ones with new personal identification numbers (PINs) and passwords.

Third, the victim should file a report with a local police department or the police department where the identity theft occurred, if that can be determined. The victim should obtain a copy of the police report should creditors need proof of the crime. Even if the thief is not apprehended, a copy of the police report may assist the victim when dealing with creditors. The victim should also file a complaint with the FTC.[85]

Fourth, certain situations may require certain additional action by the victim. For instance, if an identity thief has stolen mail, it should be reported to a local postal inspector.[86] If financial information has been obtained, the financial entity (the bank, brokerage firm, credit union, credit card company, etc.) should be contacted, the fraudulently affected accounts closed, and new accounts opened with new PINs and passwords, including affected ATM cards. Payment should be stopped on any stolen checks, and banks or credit unions should be asked to request the appropriate check verification service to notify retailers not to accept

---

[84] *See supra* notes 68-73.

[85] The FTC should be contacted on its Identity Theft Hotline at 877-IDTHEFT (438-4338), TDD at 202-326-2502, by mail at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, N.W., Washington, DC 20580, or at http://www.consumer.gov/idtheft.

[86] A phone number for the nearest postal inspection service office can be obtained from a local post office or the U.S. Postal Service Web site at http://www.usps.com/postalinspectors.

the checks.[87] If investments or securities may have been affected, brokers should be notified, and the victim should file a complaint with the SEC.[88]

If new phone service has fraudulently been established in a victim's name, or billing for unauthorized service is made to an existing account, the victim should contact the service provider immediately to cancel the account and/or calling card and open new accounts with new PINs and passwords. If a victim has difficulty removing fraudulent charges from an account, a complaint should be filed with the Federal Communications Commission (FCC).[89]

If someone is using a victim's SSN to apply for a job or to work, it should be reported to the SSA.[90] If an SSN has been fraudulently used, the IRS Taxpayer Advocates Office should be contacted.[91] The fraudulent use of an SSN might result in what appears to be an under-reporting of a victim's taxable income and an attempt by the IRS to collect taxes on the under-reported income.

If someone has fraudulently obtained a driver's license or photographic identification card in a victim's name through an office of a DMV, the local DMV should be contacted, and a fraud alert should be placed in the license. Likewise, if someone has stolen any other identification document, the entity responsible for creating the document should be contacted and informed of the

---

[87] Three check verification companies that accept reports of check fraud directly from consumers are: Telecheck, 800-710-9898; International Check Services, 800-631-9656; and Equifax, 800-437-5120.

[88] A complaint can be filed with the SEC at the SEC Enforcement Complaint Center, 450 Fifth Street, N.W., Washington, DC 20549-0202; through its Web site at http://www.sec.gov; by e-mail to enforcement@sec.gov; or by fax at 202-942-9570.

[89] A complaint can be filed with the FCC at the FCC Consumer Information Bureau, 445 12th Street, S.W., Room 5A863, Washington, DC 20554; through the FCC Enforcement Bureau Web site at http://www.fcc.gov/eb; by e-mail to fccinfo@fcc.gov; by telephone at 888-CALLFCC (225-5322); or by TTY at 888-TELLFCC (835-5322).

[90] The victim should first visit the SSA's Web site at http://www.ssa.gov, read the Guidelines for Reporting Fraud, Waste, Abuse and Mismanagement, call the SSA Fraud Hotline at 800-269-0271, and file a report with the SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235, by fax at 410-597-0118, or via e-mail to oig.hotline@ssa.gov. The victim should also call the SSA at 800-772-1213 to verify the accuracy of earnings reported under the SSN and to request a copy of the victim's Social Security statement. The statement should reveal earnings posted to the victim's SSN by the identity thief.

[91] The Internal Revenue Service Taxpayer Advocates Office can be contacted at 877-777-4778, or at http://www.treas.gov/irs/ci.

theft.[92] If someone has stolen a health insurance card, the theft should be reported to the insurer. Subsequent insurance statements should be reviewed for fraudulent billing.

If someone has fraudulently filed for bankruptcy in a victim's name, the U.S. Trustee should be contacted in the jurisdiction where the bankruptcy was filed.[93] A written complaint must be filed describing the situation and providing proof of the victim's identity. The U.S. Trustee, if appropriate, will make a referral to criminal law enforcement authorities. The victim should also file a complaint with the Federal Bureau of Investigation (FBI) in the city where the bankruptcy was filed.

In rare instances, an identity thief may create a criminal record under a victim's name by providing the victim's identity when arrested. This will cause the victim's identity to be entered into the National Crime Information Center (NCIC), which is a national computer database overseen by the FBI. Each law enforcement agency is responsible for entering their own arrest data into the NCIC database. The data can thereafter be changed only by the agency that entered the data. Consequently, victims of this type of problem should contact the FBI and request assistance in determining which law enforcement agency entered the identity information into the NCIC database. Once the identity of the law enforcement agency is determined, the victim will have to provide a sworn affidavit to the agency, attesting that it was not the victim who was arrested, etc. Some jurisdictions may require a court order authorizing any change to the NCIC database. Victims should consult an attorney to resolve the problem, as procedures for clearing one's name may vary by jurisdiction.

CONCLUSION

Identity theft was clearly identified as a serious crime a few years ago when the Identity Theft Act was passed. Since that time great strides have been made to combat the problem, but much work remains to be done. Law enforcement agencies at all levels, federal and non-federal, must work together to develop

[92] If a passport has been lost or stolen, the United States State Department should be contacted at Passport Services, Correspondence Branch, 1111 19th Street, N.W., Suite 510, Washington, DC 20036, or at http://www.travel.state.gov/passport_services.

[93] A listing of the U.S. Trustees can be found at http://www.usdoj.gov/ust.

strategies for the investigation and prosecution of offenders. At the same time, the law enforcement community must work closely with private industry to develop effective education and prevention programs. The crime of the new millennium will not fade away soon, nor will passive efforts soften the devastating impact upon its victims. Yet with hard work, cooperation, and effective communication between law enforcement and the public, identity thieves will be held accountable in this new millennium.