U.S. Department of Justice
Executive Office for United States Attorneys
United States Attorneys' USA Bulletin
March 2001 Vol. 49, No.2

Identity Theft: The Crime of the New Millennium

Sean B. Hoar

USA Bulletin

(March 2001)

Sean B. Hoar
Assistant United States Attorney
District of Oregon

The Nature of the Problem

Identity theft has been referred to by some as the crime of the new millennium. It can be accomplished anonymously, easily, with a variety of means, and the impact upon 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. *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 Comm. on Commerce*, 106th Cong. 16 (1999) (testimony of Rep. John B. Shadegg). 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 received approximately 62,000 allegations involving SSN misuse. The widespread use of

SSNs as identifiers has reduced their security and increased the likelihood that they will be the object of identity theft. The expansion and popularity of the Internet to effect commercial transactions has increased the opportunities to commit crimes involving identity theft. The expansion and popularity of the Internet to post official information for the benefit of citizens and customers has also increased opportunities to obtain SSNs for illegal purposes.

On May 31, 1998, in support of the Identity Theft and Assumption Deterrence Act, 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". The report found that methods used to obtain identity information ranged from basic street theft 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. The report also found the following: In 1995, 93 percent of arrests made by the U.S. Secret Service Financial Crimes Division involved identity theft. In 1996 and 1997, 94 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. 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. Postal Inspection investigations showed that identity fraud was perpetrated by organized crime syndicates, especially to support drug trafficking, and had a nationwide scope. 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 3,000 a month in 1992 to over 43,000 a month in 1997. 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. MasterCard stated that dollar losses relating to identity fraud represented about 96 percent of its member banks' overall fraud losses of $407 million in 1997.

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 identify 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.

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 punch in your telephone calling card number or credit card number or listen in on your conversation if 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 they are anonymously sitting in the comfort of their own home. Outside your home, thieves steal your mail, garbage, or recycling. 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 like prescription labels, or other records that bear your name, address, or telephone number.

In a recent case in the District of Oregon, 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 400 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 preapproved 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. Two of the offenders were prosecuted federally for conspiracy to commit computer fraud and mail theft under 18 U.S.C. §§1030(a)(4), 371and 1708, and consented to the forfeiture of computer equipment obtained as a result of the fraud-related activity pursuant to 18 U.S.C. § 982(a)(2)(B). One defendant was sentenced to serve a forty-one month term of imprisonment and pay $70,025.98 in restitution. United States v. Steven Collis Massey, CR 99-60116-01-AA (D.Or. 1999). The other defendant was sentenced to serve a fifteen month term of imprisonment and pay $52,379.03 in restitution. *United States v. Kari Bahati Melton*, CR 99-60118-01-AA (D.Or. 1999).

How Can Identity Theft Be Investigated and Prosecuted?

The investigation of identity theft is labor intensive and individual cases are usually considered to be too small for federal prosecution. Perpetrators usually victimize multiple victims in multiple jurisdictions. Victims often do not 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 America 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 Federal Trade Commission (FTC) to pursue effective means of prevention, investigation, and prosecution of identity theft offenses. Toward that end, workshops were recently held for the purpose of identifying the best practices to combat identity theft, including remediation, prevention, and law enforcement strategies. Workshop participants included prevention specialists, federal agency representatives, state and federal investigators, and state and federal prosecutors.

The experience of workshop participants is that law enforcement agencies at all levels, federal and non-federal, must work together investigating identity theft. Multi-agency task forces have proven successful in investigating and prosecuting identity theft. By utilizing task forces, member agencies pool scarce resources to investigate and prosecute identity theft offenses, and provide prevention training. Workshop participants also indicated that 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. One challenge is communication with victims. Communication is necessary to obtain fundamental investigative information, including loss and restitution information. In complex cases, it is imperative to devise a system for communication with the victims at the outset of the case. The AUSA should work with victim/witness units to identify the best communication system for the case. The AUSA should also work with the system administrator to develop a link from the district's web site for on-line communication with victims. The link can provide access to a data base into which victims can enter case-related information. The link can also be used to provide updates on the status of the case. Notification to the victims regarding their use of the web site can be provided through a form letter accompanying an investigative survey which must be completed, in any event, to obtain loss and restitution information.

1. 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 of which exist to assist victims in repairing their credit history. The primary identity theft statute is 18 U.S.C. § 1028(a)(7) and was enacted on October 30, 1998, as part of the Identity Theft and Assumption Deterrence Act (Identity Theft Act). 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. 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....

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. 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 $1,000 or more during any one year period is obtained. Otherwise, § 1028(b)(2)(B) provides for imprisonment of not more than three years. 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.

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. 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.

Section 1028(d)(3) 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." 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.

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. 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.

The Identity Theft Act also directed the United States Sentencing Commission to review and amend the Sentencing Guidelines to provide appropriate penalties for each offense under Section 1028. The Sentencing Commission responded to this directive by adding U.S.S.G. §2F1.1(b)(5) which provides the following:

> (5) If the offense involved -
>
> > (A) the possession or use of any device-making equipment;
> >
> > > * the production or trafficking of any unauthorized access device or counterfeit access device; or
> > > * (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.

These new guidelines take into consideration the fact that identity theft is a serious offense, whether or not certain monetary thresholds are met. For most fraud offenses, the loss would have to be more than $70,000.00 for the resulting offense level to be level 12. U.S.S.G. § 2F1.1(b)(1)(G). In providing for a base offense level of 12 for identity 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 theft offenses will usually merit a two-level increase because they often involve more than minimal planning or a scheme to defraud more than one victim. U.S.S.G. § 2F1.1(b)(2). Identity theft offenses may also provide for two to four-level upward organizational role adjustments when multiple defendants are involved. U.S.S.G. § 3B1.1

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 to refer the complaints to appropriate entities. The FTC has responded to this directive by developing a web site, great educational materials, a hotline for complaints, and a central database for information. The web site can be found at www.consumer.gov/idtheft. The hotline is 1-877-ID THEFT. Identity theft complaints are entered into Consumer Sentinel, a secure, on-line database available to law enforcement. The FTC has become a primary referral point for victims of identity theft, and a tremendous resource for these victims and law enforcement.

2. 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 (18 U.S.C. §1028(a)(1) - (6)), credit card fraud (18 U.S.C. §1029), computer fraud (18 U.S.C.§ 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. §1343), financial institution fraud (18 U.S.C. §1344), mail theft (18 U.S.C. § 1708), and immigration document fraud (18 U.S.C. § 1546). For example, computer fraud may be facilitated by the theft of identity information when stolen identity 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 U.S.S.G. § 2F1.1(c)(1) provides 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).

Several examples of how identity theft schemes may involve other statutes may be helpful. These include the case of an offender who fraudulently obtains identity information by posing as an employer in correspondence with a credit bureau. This offender might appropriately be charged with both identity theft under 18 U.S.C. § 1028(a)(7) and mail fraud under 18 U.S.C. § 1341. An offender who steals mail thereby obtaining identity information might appropriately be charged with identity theft under 18 U.S.C. § 1028(a)(7) and mail theft under 18 U.S.C. § 1708. The offender who fraudulently poses as a telemarketer thereby obtaining identity information might appropriately be charged with both identity theft under 18 U.S.C. § 1028(a)(7) and wire fraud under 18 U.S.C. § 1343.

3. 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. *United States v. Anthony Jerome Johnson*, CR 99-926 (C.D.Ca. Jan. 31, 2000).

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. *United States v. Lamar Christian*, CR 00-3-1 (D. Del. Aug. 9, 2000); *United States v. Ronald Nevison Stevens*, CR 00-3-2 (D.Del. Aug. 9, 2000).

In the District of Oregon, seven defendants have been sentenced to imprisonment for their roles in a heroin/methamphetamine trafficking organization, which included entering the UnitedStates illegally from Mexico and obtaining SSNs of other persons. The 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. 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. 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. A total of twenty-seven defendants have been convicted in the case to date, fifteen federally and twelve at the state level. *UnitedStates v. Jose Manuel Acevez Diaz*, CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *UnitedStates v. Pedro Amaral Avila*, CR 00-60044-01-HO (D.Or. Nov. 7, 2000); *United States v. Jose Arevalo Sanchez*; CR 00-60040-01-HO (D.Or. Nov. 21, 2000); *UnitedStates v. Maria Mersedes Calderon*, CR 00-60046-01-HO (D.Or. May 10, 2000); *UnitedStates v. Victor Manuel Carrillo*, CR 00-60045-01-HO (D.Or. Oct. 24, 2000); *UnitedStates v. Alfonso Flores Ramirez*, CR 00-60043-01-HO (D.Or. Aug. 30, 2000); *UnitedStates v. Cleotilde Fregoso Rios*, CR 00-60035-01-HO (D.Or. Nov. 7, 2000); *United States v. Javier Hernandez Lopez*, CR 00-60038-01-HO (D.Or. Aug. 10, 2000); *United States v. Ranulfo Salgado*, CR 00-60039-01-HO (D.Or. Jan. 18, 2001); *United States v. Angel Sanchez*, CR 00-60080-01-HO (D.Or. Aug. 31, 2000); *UnitedStates v. Cresencio Sanchez*, CR 00-60143-01-HO (D.Or. Dec. 13, 2000); *UnitedStates v. Piedad Sanchez*, CR 00-60131-01-HO (D.Or. Jan. 9, 2001); *United States v. Noel Sanchez Gomez*, CR 00-60034-01-HO (D.Or. Dec. 12, 2000); *United States v. Kelly Wayne Talbot*, CR 00-60081-01-HO (D.Or. Dec. 31, 2000); *United States v. Jose Venegas Guerrero*, CR 00-60037-01-HO (D.Or. Nov. 21, 2000); *State of Oregon v. Fred Harold Davis*, Case No. 006276FE (Jackson County Dec. 13, 2000); *State of Oregon v. Pablo Macias Ponce*, Case No. 004317MI (Jackson County Sept. 13, 2000); *State of Oregon v. Raul Navarro Guiterrez*, Case No. 005257FE (Jackson County Nov. 8, 2000); *State of Oregon v. Miranda Mae Byrne*, Case No. 004363FE (Jackson County Jan. 9, 2001); *State of Oregon v. James Tracy Campbell*, Case No. 002376FE (Jackson County Oct. 18, 2000); *State of Oregon v. Ann Marie Eaton*, Case No. 002378FE (Jackson County Aug. 25, 2000); *State of Oregon v.*

Michael Scott Gilhousen, Case No. 002225FE (Jackson County Nov. 7, 2000); *State of Oregon v. Robert Dean Golden*, Case No. 002726FE (Jackson County Oct. 18, 2000); *State of Oregon v. Annetta Lynn Kelley*, Case No. 002377FE (Jackson County July 24, 2000); *State of Oregon v. Gerald Jerome King*, Case No. 003594FE (Jackson County Oct. 31, 2000); *State of Oregon v. Micah John Right*, Case No. 002374FE (Jackson County Sept. 7, 2000); and *State of Oregon v. Todd Ivan Williams*, Case No. 004533FE (Jackson County Jan. 12, 2001).

4. Federal Credit Laws

It is important for training purposes and to assist victims in repairing damage to their credit history that prosecutors have at least a cursory understanding of credit laws that impact identity theft. The Fair Credit Reporting Act establishes procedures and time frames for correcting mistakes on credit records and requires that your record only be provided for legitimate business, credit, or employment needs. 15 U.S.C. § 1681 *etseq.* The Truth in Lending Act limits liability for unauthorized credit card charges in most cases to $50.00. 15 U.S.C. § 1601 *et seq.* The Fair Credit Billing Act establishes procedures for resolving billing errors on credit card accounts *if* the unauthorized charge is reported within certain time frames. 15 U.S.C. § 1666. 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. 15 U.S.C. § 1692. The Electronic Fund Transfer Act provides consumer protections for transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers if the unauthorized transfer is reported within certain time frames. 15 U.S.C. §1693. 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 $50.00. If reported after two business days but within 60 days of the first statement showing an unauthorized transfer, the losses are limited to $500.00. Otherwise, losses may only be limited by the amount obtained. 15 U.S.C. § 1693(g)(a).

5. State Criminal Laws

Most states have laws prohibiting the theft of identity information. Where specific identity theft laws do not exist, the practices may be prohibited under other state laws or the states may be considering such legislation. The following is a list of current state laws which prohibit the theft of identity information: Ariz. Rev. Stat. §13-2008; Ark. Code Ann. § 5-37-227; Cal. Penal Code § 530.5; 2000 Colo. Legis. Serv. ch 159 (May 19, 2000); 1999 Conn. Acts 99-99; Del. Code Ann. tit. 11, § 854; Fla. Stat. Ann. §817.568; Ga. Code Ann. § 16-9-121 to 16-9-127; Idaho Code § 18-3126; 720 Ill Comp.Stat. 5/16G; Ind.Code § 35-43-5-4 (2000); Iowa Code § 715A.8); Kan. Stat. Ann. § 21-4018; Ky. Rev. Stat. Ann. § 514.160; La. Rev. Stat. Ann. § 67.16; Me. Rev. Stat. Ann. tit. 17-A, § 354-2A; Md. Ann. Code art. 27, § 231; Mass. Gen. Laws ch. 266, § 37E; Minn. Stat. Ann. § 609.527; Miss. Code Ann. § 97-19-85; Mo. Rev. Stat. § 570.223; Neb. Rev. State. § 28-101; Nev. Rev. Stat. §205.465; N.H. Rev. Stat. Ann. § 638:26; N.J. Stat. Ann. § 2C:21-17; N.C. Gen. Stat. §14-113.20; N.D. Cent. Code § 12.1-23-11; Ohio Rev. Code Ann. 2913.49; Okla. Stat. tit. 21, §1533.1; Or. Rev. Stat. § 165.800; Pa. Cons. Stat. Ann. § 420; R.I. Gen. Laws § 11-49.1-1; S.C. Code Ann. § 16-13-500; S.D. Codified Laws 20; Tenn. Code Ann. § 39-14-150; Tex. Penal Code Ann.§ 35.51; Utah Code Ann. § 76-6-1101-1104; VA. Code Ann. § 18.2-186.3; Wash. Rev. Code §9.35; W. Va. Code Ann. § 61-3-54; Wis. Stat.

§943.201; Wyo. Stat. Ann. § 6-3-901.

How Can Identity Theft Be Prevented?

While it is extremely difficult to prevent identity theft, the best approach is to be proactive and take steps to avoid becoming a victim. As prosecutors, it is important to learn how to prevent identity theft in order to provide training to law enforcement and private industry. We can also complement the assistance to victims provided by our victim/witness units. A thorough guide to preventing and responding to identity theft can be found in Mari Frank and Beth Givens, *Privacy Piracy! A Guide to Protecting Yourself from Identity Theft*, Office Depot, (1999). Related information can be found at www.identitytheft.org. The FTC has also published a helpful guide entitled FTC, *ID Theft: When Bad Things Happen to Your Good Name*, (August 2000). This and related information can be found at 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*.

1. 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 a SSN if doing a credit check for purposes of financing a purchase. Some entities, however, may simply want the SSN for record-keeping purposes. Businesses may choose to not provide a service or benefit without obtaining a person's SSN, but the choice as to whom a SSN is provided should be exercised with caution. In the event an entity, such as a hospital or a Department of Motor Vehicles (DMV), assigns a SSN as a patient or client identification number, the customer should request that an alternative number be assigned.

2. 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.

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

According to the FTC Identity Theft Clearinghouse, the primary means for thieves to obtain identity information is through the loss or theft of purses and wallets. 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 a 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 safety 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.

4. Secure Your Mailbox.

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

5. 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 the entity with whom they are doing business. In addition to cautiously choosing with whom identity information is shared, computer users should install a firewall on their personal computers to prevent unauthorized access to stored information. 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. A firewall is especially necessary 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.

6. 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.

7. Shred Nonessential Material Containing Identity Information.

All nonessential documentary material containing any type of identity information should be shredded prior to being placed in garbage or recycling. The term "nonessential" 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.

8. "Sanitize" the Contents of Garbage and Recycling.

All nonessential 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 gold mine when obtained by an identity thief.

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

10. Remove Your Name from Mailing Lists.

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 state agencies, market identity information of customers unless a request is received, in writing, that such information is not to 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.

To opt out of the mailing lists of the three major credit bureaus (Equifax, Experian, and Trans Union), call 1-888-5OPT-OUT. To opt out of many national direct mail lists, write the Direct Marketing Association, DMA Preference Service, P.O. Box 9008, Farmingdale, N.Y. 11735-9008. To opt out of many national direct e-mail lists, visit 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, N.Y. 11735-9014.

11. 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.

12. Periodically Request Copies of Credit Reports.

Credit reports are available for $8.00 from the three major credit bureaus (Equifax, Experian, and Trans Union). 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 unauthorized accounts have been opened or unauthorized changes made to existing accounts.

To order a report from Equifax, visit www.equifax.com, call 1-800-685-1111 or write P.O. Box 740241, Atlanta, GA 30374-0241. To order a report from Experian, visit www.experian.com, call 1-888-EXPERIAN (397-3742) or write P.O. Box 949, Allen, TX 75013- 0949. To order a report from Trans Union, visit www.tuc.com, call 800-916-8800 or write P.O. Box 1000, Chester, PA 19022.

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 of 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. 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. The reports should be reviewed carefully to identify unauthorized accounts or unauthorized changes 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 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.

To report fraud to Equifax, visit www.equifax.com, call 1-800-525-6285 and write P.O. Box 740241, Atlanta, GA 30374-0241. To report fraud to Experian, visit www.experian.com, call 1-888-EXPERIAN and write P.O. Box 949, Allen TX 75013-0949. To report fraud to Trans Union, visit www.tuc.com, call 1-800-680-7289 and write Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634.

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 companies and other utilities, and 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. 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 in the event 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. The FTC should be contacted on its Identity Theft Hotline toll free at 1-877-ID THEFT (438-4338), TDD at 1-202-326-2502, by mail at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, or at www.consumer.gov/idtheft.

Fourth, certain situations may require additional action by the victim. For instance, if an identity thief has stolen mail, it should be reported to a local postal inspector. 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 www.usps.com/postalinspectors. 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 the checks. Three check verification companies that accept reports of check fraud directly from consumers are: Telecheck: 1-800-710-9898; International Check Services: 1-800-631-9656; and Equifax: 1-800-437-5120. If investments or securities may have been affected, brokers should be notified and the victim should file a complaint with the Securities and Exchange Commission (SEC). A complaint can be filed with the SEC at the SEC Enforcement Complaint Center, 450 Fifth Street, NW, Washington, D.C. 20549-0202; its web site www.sec.gov, e-mail enforcement@sec.gov, or fax (202) 942-9570.

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). A complaint can be filed with the FCC at the FCC Consumer Information Bureau, 445 12th Street, S.W., Room 5A863, Washington, DC 20554; the FCC Enforcement Bureau web site www.fcc.gov/eb, e-mail fccinfo@fcc.gov, telephone 1-888-CALL FCC, or TTY 1-888-TELL FCC.

If someone is using a victim's SSN to apply for a job or to work, it should be reported to the Social Security Administration (SSA). The victim should first visit the SSA's web site at www.ssa.gov, read the Guidelines for Reporting Fraud, Waste, Abuse and Mismanagement, and then call the SSA Fraud Hotline at 1-800-269-0271, and file a report at SSA Fraud Hotline, P.O. Box 17768, Baltimore MD 21235, fax 410-597-0118 or e-mail oig.hotline@ssa.gov. The victim should also call the SSA at 1-800-772-1213 to verify the accuracy of earnings reported under the SSN and to request a copy of the victim's Social Security Personal Earnings and Benefit Estimate Statement. The Statement should reveal earnings posted to the victim's SSN by the identity thief. If an SSN has been fraudulently used, the Internal Revenue Service (IRS) Taxpayer Advocates Office should be contacted. The fraudulent use of an SSN might result in what appears to be an underreporting of a victim's taxable income and an attempt by the IRS to collect taxes on the underreported income. The IRS Taxpayer Advocates Office can be contacted at 1-877-777-4778 or www.treas.gov/irs/ci.

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 theft. If a passport has been lost or stolen, the United States State Department should be contacted at Passport Services, Correspondence Branch, 1111 19th Street, NW, Suite 510 Washington, DC 20036, or www.travel.state.gov/passport_services.html. 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 region where the bankruptcy was filed. A listing of the U.S. Trustees can be found at www.usdoj.gov/ust. 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 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 identity when arrested. Victims of this type of problem should contact the FBI and initiate a request that the victim's name be cleared, and retain 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 two 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 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.

ABOUT THE AUTHOR

Sean B. Hoar has been an AUSA since 1991 and is the Computer and Telecommunications Coordinator (CTC) for the southern half of the District of Oregon. As such, he prosecuted the first case in the United States under the No Electronic Theft Act (NET Act) involving criminal copyright infringement on the Internet. He is primarily concerned with developing partnerships with local, state and federal law enforcement agencies to prevent, investigate and prosecute cyber crime. Previously he was primarily involved in the prosecution of organizational narcotics traffickers and received the Directors Award for his role in prosecuting a heroin trafficking organization based in Southeast Asia which included a General in the Royal Thai Army who was a member of the Supreme Command of the Royal Thai Armed Forces.

###

- **More information on: Prosecuting Crimes Facilitated by Computers and by the Internet**

Go to . . . CCIPS Home Page || Justice Department Home Page
