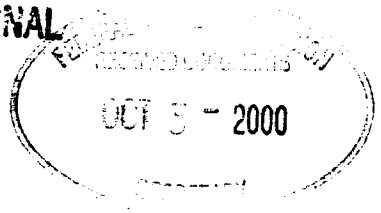
CALIFORNIA STATE UNIVERSITY
NORTHRIDGE

Department of Business Law
College of Business Administration and Economics

ORIGINAL



September 28, 2000

Secretary, Federal Trade Commission
Room H-159
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Sir or Madam:

Please find enclosed reprints of an article entitled, "Deterring Identity Theft in the Information Age: The Identity Theft and Assumption Deterrence Act," which Professor Bruce Zucker and I recently published in the Cornell Journal of Law & Public Policy. The article was also reprinted in the International Review of Computer Law, and appears online at <http://www.bileta.ac.uk/99papers/saunders.htm>.

I am submitting this article for use or distribution at the upcoming Identity Theft Victim Assistance Workshop. While I realize that the deadline has passed to request to participate as a panelist, I would be glad to attempt to arrange my schedule to participate if invited. In any event, however, I hope that the article is of use to you and of interest to those who attend the workshop.

Yours very truly,

Kurt M. Saunders
Assistant Professor

Enclosures

18111 Nordhoff Street · Northridge · CA · 91330-8375 · phone (818) 677-2905 · fax (818) 677-6264 · e-mail Business.law@csun.edu · http://www.csun.edu

INTERNATIONAL REVIEW OF LAW COMPUTERS
& TECHNOLOGY, VOLUME 13, NO. 2, PAGES 183–192, 1999

Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act

KURT M SAUNDERS and BRUCE ZUCKER

ABSTRACT *The advent of the information age has created new challenges to the ability of individuals to protect the privacy and security of their personal information. One such challenge is that of identity theft, which has imposed countless hardships upon its victims. Perpetrators of this fraud use the identities of others to steal money, obtain loans, and generally violate the law. The Identity Theft and Assumption Deterrence Act of 1998 makes the theft of personal information with the intent to commit an unlawful act a federal crime in the United States with penalties of up to 15 years imprisonment and a maximum fine of $250,000. The Act designates the Federal Trade Commission to serve as an advocate for victims of identity fraud. This article first examines the problem of identity fraud and the inadequacy of existing remedies, and then assesses the need for and likely impact of the Act, as well as issues relating to the effectiveness of its future enforcement.*

Introduction

> **identity,** n; ... 2. (a) the condition or fact of being some specific person ... ; individuality; (b) the condition of being the same as ... someone assumed, described, or claimed.[1]

With the emergence of the Internet and the increasing number of commercial transactions facilitated electronically, personal information is flowing throughout the country and around the world at speeds never before imagined. As a consequence, tax identification numbers, Social Security numbers, driver's license information, fingerprints, and similar private and confidential information are now more accessible than ever before. An immense quantity of such information is often stored on-line in computer databases,[2] on proprietary networks of credit reference services, and on the Internet.[3] How can such information be misused?

Consider the following scenario. Having impeccable credit, a person decides to purchase a new car at a local car dealership. Intending to finance the purchase through

Correspondence: Kurt M. Saunders and Bruce Zucker, Faculty of Law, California State University, Northridge, USA.

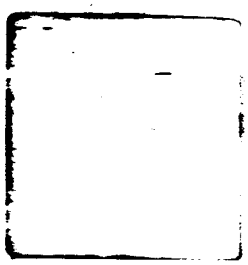
1369-0869/99/020183-10

credit arranged by the dealer, he completes a standard application form. After conducting a credit check, he is told that his credit application was denied. After further inquiry, he discovers that the credit reporting agency lists him as having 26 open lines of revolving credit and three different car loans. Further, he discovers that it lists eight different residences over the past year. Even though he believes that he has never made a delinquent payment, almost every one of his creditors reports him in default.

There is one problem—he never opened any of these credit lines himself. Someone obviously stole his identity and used his perfect credit to obtain tens of thousands of dollars worth of goods and services. After exhausting his credit limit, these con-artists move on to the next unwitting victim, leaving this person and his ruined credit in their wake.[4] What, if anything, can he do next?

Described as the neoteric crime of the information technology era, identity theft is the illicit use of another individual's identifying facts (name, birth date, Social Security number, address, telephone number, or other similar information) to perpetrate an economic fraud, such as opening a bank account, obtaining credit, applying for bank or department store cards, or leasing cars or apartments in the name of another.[5]

According to some reports, an estimated 40,000 people in the United States fall victim to such crimes each year.[6] Authorities estimate that identity theft imposes a cost on consumers approaching $100 million annually.[7] The United States Secret Service, which tracks major identification theft cases, reports that the dollar value of such cases has nearly doubled in the last year, and the Social Security Administration has seen a threefold increase in improper use of Social Security numbers. According to credit reporting firms, fraud reports have climbed from less than 12,000 annually in 1992 to more than 500,000 currently.[8]



Using readily available technology, perpetrators of identity crimes typically break into computer databases containing personal identification information. Other times, they simply copy or modify fingerprints recorded or transmitted electronically.[9] In a prepared statement presented to Congress on this issue, the Federal Trade Commission illustrated other such means with which identity thieves carry out their schemes:

> Historically, identity thieves have accomplished their crimes through simple means—pickpocketing wallets, stealing pre-approved credit applications from mailboxes, or raiding trash dumpsters for discarded receipts and files. Recently, more sophisticated schemes are gaining popularity. One such method is securing low-level employment with a financial institution or other entity that gives the perpetrator access to consumer credit reports or other identifying data, for their personal exploitation or for use by organized identity theft rings. For example, one fraud ring used such credit reports quickly to acquire fake I.D. cards, open 'instant credit' accounts, and then run up thousands of dollars in debt. A recent case brought by the United States Secret Service demonstrates how computer-savvy identity thieves may exploit information available over the Internet. In that case, the defendants were a Maryland couple who pled guilty in September 1997 to running up debt exceeding $100,000 under their stolen identities. They admitted to routinely using Internet databases to select their victims.[10]

This article examines the problems created by identity theft and explores recently enacted federal legislation intended to further proscribe it and offer assistance to its

victims. It first considers the nature and role of identity in society, including the inadequacy of existing statutory and common law to prohibit and redress identity theft. It discusses the material provisions of the Identity Theft and Assumption Deterrence Act of 1998 and assesses its probable effect on enforcement. Finally, it presents observations and comments of these authors as to its likely impact on curtailing such crime and discusses some suggestions for effective enforcement.

The Importance of Identity in Society and Electronic Commerce and the Role of the Law in its Protection

Identity, Authentication, and Privacy of Personal Information

The notion of identity is inseparable from a person's intrinsic nature and sense of individuality. Among other things, it relates to a person's conscious sense of 'self' and individuality, while also allowing others to recognize or distinguish him or her from others.[11] In society, the concept of identity is broader than merely knowing a person's name or recognizing a person's face. Rather, the identity of a person is often separate from his or her attributes and physical traits. In many instances, to learn or establish the identity of a person involves reference to some set of institutional or socially agreed upon identifiers that authenticates a person's uniqueness in relation to others.

Likewise, a person's identity, as well as the ability to prove it, is fundamental to many commercial and institutional transactions. For instance, businesses need to be assured that the person signing a contract or accepting delivery of goods is in fact who he says he is. Banks may require proof that the person who telephones to request information about her account or appears to make a withdrawal is in fact the same person who opened the account. In order to evidence identity, many institutions have resorted to systems that employ identifiers—such as Social Security or telephone numbers, mother's maiden names, or birth dates—that are not necessarily unique or that may be easily discovered. They may issue identification devices—such as driver's licenses or membership cards—that may be readily stolen or duplicated. Sometimes, one institution or entity may use an identifier issued by another institution or entity as a means of establishing or authenticating a person's identity. This occurs, for example, when an airline or tavern requires production of a government-issued photo identification.

Nevertheless, these apparently reliable solutions provide easy opportunities for corruption, fraud, and error.[12] These problems, however, have been further exacerbated by the emergence of information technologies such as computerized databases and networks that can facilitate commercial and institutional transactions between parties separated by great distance or known to one another solely through the use of pseudonyms.[13] In such an environment, the opportunities for corruption, identity fraud, and error are substantially increased. Indeed, the emergence of the Internet as a potential new marketplace has underscored the need to establish secure and reliable channels of electronic commerce for identity authentication. Presently used identity authentication procedures make use of passwords, data encryption systems, digital signatures, and firewalls, alone or in combination,[14] in order to ensure trust and confidentiality in the agreement formation process.[15]

The unfortunate story of Terry Rogan, the plaintiff in *Rogan* v *City of Los Angeles*,[16] illustrates how identity theft and inaccuracy of electronically stored information may turn into an ordeal. In 1981, McKandes, an escapee from an Alabama state prison, began using Rogan's name after he obtained a copy of Rogan's birth certificate in Michigan. McKandes

then relocated to California and used Rogan's birth certificate to obtain a driver's license and other identification documents in Rogan's name. In early 1982, McKandes, who was still using Rogan's identity, was arrested by the Los Angeles Police Department (LAPD) on suspicion of murder, but was later released. Several months later, an arrest warrant was issued in the name of 'Terry Dean Rogan,' charging him with two robbery-murders which had occurred in Los Angeles. The warrant information was entered into a national computer criminal information database known as the National Crime Information Center (NCIC), ensuring that every police officer in the United States would have access to and could thereby become aware of the outstanding warrant in the name of Rogan which was outstanding in California. Information containing McKandes' physical characteristics and fingerprints was added in June 1982.

In October 1982, Rogan was arrested on suspicion of trespass by police in Saginaw County, Michigan. The Michigan police discovered the robbery-murder warrant when they made an inquiry of the NCIC database; however, a comparison of Rogan's fingerprints and physical characteristics with those recorded in NCIC established that he was not the suspect wanted by the LAPD. Although the NCIC information about Rogan was automatically removed after his October arrest, the LAPD reentered the same information containing Rogan's name in November 1982. In early 1983, Rogan's car was stopped by the county sheriff's deputies in Saginaw, Michigan for failure to use a turn signal.

When the robbery-murder warrant information was received during the routine computer check, Rogan was ordered out of his car at gunpoint, searched, handcuffed, and taken into custody. While in jail, he was handcuffed to the metal bars of his cell while the police contacted the LAPD and the Saginaw police. Rogan was released 2 hours later when his identity was clarified.

Later in 1983, Rogan was again stopped for a traffic offense and detained due to the inaccurate NCIC information, but later released. In July 1983, Rogan was driving from Michigan to Oklahoma to visit relatives when he was stopped by Texas police for speeding, arrested at gunpoint and handcuffed on the basis of the NCIC information, held in jail pending an investigation of his true identity, and then released. This process was repeated yet again in January 1984 when Rogan was stopped in Saginaw, Michigan by a deputy sheriff for driving without headlights. Finally, after that incident, the LAPD removed the NCIC record in Rogan's name.

Rogan brought suit against the City of Los Angeles under 42 U.S.C. §1983 for deprivation of his constitutional rights due to the use of incorrect and incomplete criminal information in an arrest warrant.[17] The court held that the LAPD's use of the NCIC database was grossly negligent and awarded judgment to Rogan as a matter of law for the pain and humiliation suffered as a result of his experience.[18]

The Inadequacy of Existing Law and the Need for New Legislation

Fundamental notions of fairness and equity would suggest that the legal system would have already criminalized identity fraud. However, it has not. Under federal law, an individual who illegally obtains, uses, or transfers false *identification* commits a felony.[19] However, nothing in the existing federal statutory scheme specifically prohibits a person from illegally assuming the identity of another individual without first obtaining false documents but with the intent to engage in fraud-related activity. Moreover, the United States Secret Service, which investigates and prosecutes only a small portion of these cases under the federal mail and wire fraud statutes.[20] This is due to the fact that many of these crimes

involve such small amounts that they are too insignificant to justify use of investigative and prosecutorial resources.[21] As discussed above, many of these identity thefts occur without the thief ever obtaining a single identification document since the fraud may result entirely from the appropriation of identifying information publicly available in databases on the Internet or elsewhere.[22]

Likewise, tort law does not appear to provide an adequate remedy. The intentional tort of conversion, which is the civil law equivalent of theft, affords no remedy because the defendant must acquire and deprive the plaintiff of his or her property without permission. No court has as yet classified a person's identity as tangible personal property; however, most courts have recognized a property right connected with a person's image and likeness and his or her ability to control it known as the 'right of publicity'.[23] The tort of fraud, which occurs when a defendant makes a misrepresentation of fact in order to induce another to act in reliance upon it,[24] is of no use to a victim of identity theft. A misrepresentation is fraudulent if the defendant knows or believes that the matter is not what he or she represents it to be.[25] Liability for this wrongful conduct, however, is to the person who suffered a pecuniary loss due to his or her justifiable reliance upon the misrepresentation.[26] As such, under this theory, only the victim of the fraud itself, rather than the victim of identity theft, would have recourse against the defendant.

The type of invasion of privacy known as appropriation of name or likeness might also seem to offer relief. Invasion of privacy by appropriation of name or likeness occurs when the defendant appropriates the plaintiff's name or image without consent for the defendant's own advantage.[27] This tort is not concerned with pirating the plaintiff's name *per se*, but with taking the plaintiff's name for the defendant's *commercial* advantage, such as 'to advertise the defendant's product, or to accompany an article sold, to add luster to the name of a corporation, or for other business purposes'.[28] Thus, there is no liability under this theory unless the plaintiff's identity has been used without permission for purposes of trade or commerce, rather than merely for the defendant's personal pecuniary benefit.

As to the protection of information itself, including data that may be used to establish or authenticate identity, existing law focuses upon concerns of security and privacy. Various federal statutes restrict the accumulation, storage, and distribution of information; other laws are designed to ensure that the information stored and distributed is accurate.[29] The Privacy Act, for example, regulates the maintenance and disclosure of personal data and personally identifiable information held by the federal government.[30] The Computer Fraud and Abuse Act imposes criminal penalties for the intentional and unauthorized access to government and federal interest computers for the purpose of altering, damaging, or destroying information.[31] Under the Electronic Communications Privacy Act, criminal sanctions are imposed for unauthorized interception or disclosure of, as well as unauthorized access to, electronic communications stored in a facility involved in electronic communications services and for knowingly divulging the content of such communications while in storage.[32] While they have aided in limiting the threat of a dramatic decrease in privacy and an inevitable increase in losses due to inaccurate information, these laws provide little or no relief for the victims of identity theft and misuse.[33]

In addition, federal consumer credit protection statutes provided limited assistance to victims of identity fraud. For instance, the Fair Credit Reporting Act regulates the collection and use of personal data by credit reporting agencies by prohibiting disclosure of consumer credit reports without consent unless such disclosure is made for a legitimate business reason.[34] The Truth-in-Lending Act, enacted in 1968, is primarily a disclosure law that requires sellers and lenders to fully disclose credit or loan terms to debtors.[35] One

amendment to the Truth-in-Lending Act, known as the Fair Credit Billing Act, limits the liability of credit cardholders to $50 per card for unauthorized charges made before the credit card issuer is notified that the card has been lost or stolen.[36] The use of a credit card is unauthorized only when it is used without the permission or approval of the cardholder.[37]

The Identity Theft and Assumption Deterrence Act

In 1997, Senator Jon Kyl (R-Arizona) introduced Senate Bill 512, known commonly as the Identity Theft and Assumption Deterrence Act. It was passed by Congress in October 1998 and was signed by President Clinton on October 30, 1998.[38] The intent of the Act is to expressly criminalize identity theft, classify private citizens as direct victims of such conduct, and allow courts to include loss suffered by individual consumers into restitution orders for expenses resulting from rectifying their credit records. In addition, the Act directs the United States Sentencing Commission[39] to incorporate the crime of identity theft into the appropriate sections of the United States Sentencing Guidelines Manual[40] and to select the appropriate corporal and financial sanction for federal judges to use at sentencing.

The Act amends Title 18 of the United State Code to specifically criminalize identity theft. As enacted, 18 U.S.C. §1028(a) (Fraud and Related Activity in Connection with Access Devices) will add the following pertinent language:

> Whoever knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or otherwise promote, carry on, or facilitate any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law, [commits identity theft].[41]

The Act defines 'means of identification' as someone who steals any name or number that may be used to identify a specific individual.[42] It designates the maximum penalty for each violation of this section as 15 years imprisonment, a $250,000 fine, a 3-year period of supervised release, and a special assessment of $100.

Under current law, the federal courts are precluded from awarding restitution to individuals who incur expenses associated with the theft of their identities. If, for example, an individual spent several thousand dollars in attorney fees in order to correct his credit history, to deal with various creditors affected by the identity theft, or to clear his reputation, the federal courts could not award restitution of these expenses because this individual would not be considered a 'victim ... directly and proximately harmed as a result of the commission of [the offense]'.[43] Only direct victims of the fraudulent activity (such as banks, merchants, or other such entities ultimately responsible for rectifying the damage) could receive awards of restitution.[44]

Consequently, the Act amended 18 U.S.C. §3663A (Mandatory Restitution to Victims of Certain Crimes) so as to actually *mandate* the federal courts to order restitution for consumer victims. As defined in the Act, restitution includes 'any costs, including attorney fees, incurred by the victim, including any costs incurred in clearing the credit history or credit rating of the victim; or in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as a result of the actions of the defendant'.[45]

Additionally, the Act instructs the United States Sentencing Commission to amend the United States Sentencing Guidelines to include the concept of 'identity theft' into the

relevant fraud-related guideline sections. The Act gives the Sentencing Commission broad discretion in how to carry out this mandate,[46] but does order it to consider, *inter alia*, the extent to which the number of victims were involved in the offense, the harm to a victim's reputation, a victim's inconvenience and other difficulties resulting from the offense, the number of identification documents used by the perpetrator, and the extent to which the value of the loss to any individual caused by the offense is somehow an inadequate measure of appropriate penalty.

The last portion of the Act directs the Federal Trade Commission (FTC) to establish a centralized clearinghouse to record and track complaints and to provide consumer education service for victims of identity theft. Finally, the Act instructs the FTC to implement procedures for referring complaints to the three major national consumer-reporting agencies (Equerian/TRW, Transunion, and Equifax) and to channel them to the respective law enforcement agencies for investigation.

The Impact of the Act

The Identity Theft and Assumption Act accomplishes three main objectives: first, it ensures private consumers who fall victim to an identity theft have standing as victims in federal criminal cases and forces the courts to consider damage to these consumers and include them when fashioning restitution orders. Second, the Act provides for stiffer penalties for perpetrators of this crime[47] and implements certain procedures for investigation and enforcement.[48] Third, it directs the Federal Trade Commission (FTC) to establish procedures for educating the public, receiving complaints, and coordinating enforcement efforts with various investigatory agencies.[49]

With respect to the first objective, victims will have enforceable restitution orders with which to attempt to get reimbursement. However, like many judgments entered against defendants who are involved in unscrupulous activity, such individuals are often difficult to trace or find, judgment proof, and without assets or income. The chance of these victims actually receiving any compensation from the restitution orders is minimal.

Regarding the second objective, the Sentencing Commission may choose to enact harsh penalties for such conduct. Under the current system, perpetrators of fraud receive sentencing enhancements in direct correlation with the amount of loss caused by their activities,[50] the amount of planning involved,[51] if a jointly undertaken activity, the level of sophistication of the role the perpetrator played,[52] the susceptibility and status of the victims,[53] and the number of victims involved in the offense.[54] Depending upon the composition of the Sentencing Commission,[55] it could enact a relatively harsh guideline for the imposition of punishment for offenders of identity theft.[56] In order to ensure satisfactory consideration of the various factors detailed in the Act, and considering the rather unique nature and consequences of identity theft as it compares to other theft and fraud-related crime, it would be appropriate for the Commission to establish a separate guideline section to either Part B (Offenses Involving Property) or Part F (Offenses Involving Fraud or Deceit) rather than incorporate it into one of the existing guideline sections.[57]

As to the third objective, the Act makes clear that the FTC is the primary agency responsible for its implementation and coordination of enforcement. Congress directed the FTC to educate the public on identity theft, receive and document reports of such illicit conduct, coordinate any complaints by consumers of identity theft with law enforcement, and establish procedures for the public to file complaints.[58] The Act gives the FTC 1 year

to accomplish these three primary tasks. However, nothing in the Act provides for a periodic assessment of the success of implementation or for the FTC to report to Congress whether it is in compliance with these directives. There appears to be a need for such assessment procedure.

Conclusion

With the onset of the information age, the fundamental ability to protect one's personal information and identity is now more in jeopardy than ever. The widespread use of computer databases and the Internet to store and transmit information have made identity theft even easier to perpetrate. Indeed, empirical studies indicate that the number of crimes related to identity theft is steadily increasing, with enormous cost to the victims. Surprisingly, the states have not acted to proscribe this misconduct, which often involves interstate commerce, and identity theft had not been specifically banned by federal legislation until the present time. However, the enactment of the Identity Theft and Assumption Deterrence Act of 1998 specifically criminalizes identity fraud and empowers the federal courts to award consequential damages to victims of such crimes.

When President Clinton signed the Act into law, he said 'as we enter the information age, it is critical that our newest technologies support our oldest values'.[59] Implementation of this Act will empower law enforcement, consumer protection agencies, and the public to combat identity thieves and deter such conduct as society continues to see the expansion of advanced technology.

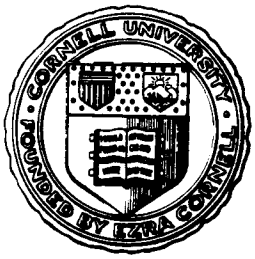
Notes and References

1. *Webster's New Twentieth Century Dictionary* 902, 2nd edn, 1983.
2. The Department of Health and Human Services, the Selective Service System, and the Internal Revenue Service all cross-reference information using Social Security numbers. As a result, 'anyone who knows an individual's SSN can amass a wealth of highly sensitive information about that individual' (G B Trubow, 'Protecting informational privacy in the information society' 10 N. Ill. U.L. Rev. 521, 526 (1994).
3. Indeed, the Internet is a veritable treasure trove of personal information where, starting with a person's name and address, one can find out, in a relatively short amount of time, 'what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house and how much taxes you pay on it'(J Quittner 'Invasion of privacy' *Time*, 25 August 1997, at 33 (quoting C Lane *Naked in Cyberspace: How to Find Personal Information Online*, 1997). See also *The Stalker's Home Page: A Stalking We Go!* (visited 8 December 1998) <http://www.glr.com/stalk.html> (listing hyperlinks to web sites containing addresses, phone numbers, Social Security numbers, property taxes, and similar information).
4. For other illustrations of hardships suffered by victims of identity theft, see, e.g., E Hendricks 'Identity theft key to major medical fraud operation' *Privacy Times*, 6 February 1998, at 3–4; 'Are You a target for identity theft?' *Consumer Reports*, Vol 62, No 9, September 1997, at 11; L Fickenscher 'Credit industry strains to stem tide of identity theft' *American Banker*, 14 October 1996, at 12; B McMenamin 'Invasion of the credit snatchers' *Forbes*, 26 August 1996, at 258; 'An identity crisis, an identity crisis' *Chicago Tribune*, 24 September 1996, §C ('Your money') at 7; R Lemos 'Identity theft a big business' *ZDNet News*, 15 April 1998 (visited 8 December 1998) <http:/;s hwww.zdnet.com/zdnn/0414/306824.html>.
5. M Grossman 'The other you: the misery of identity theft' *Broward Daily Business Review*, 4 September 1998, at B1.

6. 'Identity theft: how to take steps to clear your name' *Orange County Register*, 23 August 1998, at K4.
7. Grossman, *supra* note 3, at B1.
8. K M Kristof 'New law to assist victims in fight against identity fraud' *Los Angeles Times*, 31 October 1998, at C1.
9. Theft and misuse of biometric identification data, including voice, retinal, and facial prints, are increasing in frequency. See, e.g., R Lemos 'Protecting your digital ID' *ZDNet News*, 13 February 1998, at <www.zdnet.com/zdnn/0213/285183.html>.
10. *Prepared Statement of the Federal Trade Commission on 'Identity Theft' Before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary*, 105th Cong. 3 (1998) (statement of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission). See also Official Transcript of 'FTC Consumer Identity Fraud Meeting', 20 August 1996 at 12–13 (visited 8 December 1998) <http://www.ftc.gov/ftc/conferences.htm>. The Federal Trade Commission maintains a privacy page at its web site to advise consumers how to protect personal information and how to obtain assistance in the event if they are victimized by identity theft. <http://www.ftc.gov/privacy/index.html>.
11. For an extensive treatment of the concept of 'identity' in its social and cultural context, see, generally, E H Erikson, *Identity and the Life Cycle*, W W Norton & Co, New York, 1980.
12. V Ellis 'Thriving trade in fake drivers' licenses poses tough problem for DMV *Los Ange les Times*, 5 April 1998, at A1 and A26.
13. Closely related to the issue of identity protection is the issue of whether *anonymity* in electronic communications should be legally guaranteed as a matter of free speech and privacy. See A M Froomkin 'Anonymity and its enmities'1995 *J. Online L.*, art 4 <http://www.law.cornell.edu/jol/jol.table.html>.
14. These security methods are discussed in S Garfinkle & G Stafford, *Web Security and Commerce*, 1997.
15. See J K Winn 'Open systems, free markets, and regulation of Internet commerce' 72 Tul. L. Rev. 1177, 1998; M D Ford 'Identity authentication and "E-Commerce" ' 1998(3) *J. Info. L. & Tech.* (visited 8 December 1998) <http://www.law.warwick.ac.uk/jilt/98–3/ford.html>; A Ferraro 'Electronic commerce: the issues and challenges to creating trust and a positive image in consumer sales on the World Wide Web' *First Monday* Vol 3, No 6, 1998 (visited 8 December 1998) <http://www.firstmonday.dk/issues/issue3_6/ferrero/index.html>.
16. 668 F. Supp. 1384 (C.D. Cal. 1987).
17. *Idem*, at 1386–1387.
18. *Idem*, at 1391.
19. 18 U.S.C. §1029.
20. *Idem*, §§1341 and 1343.
21. 83 Cong. Rec. H9993–H9998 (daily ed. 14 October 1998) (statement of Rep. McCollum).
22. *See supra*, notes 2–4, 6, and accompanying text.
23. *Idem*, §525.
24. *Idem*, §525.
25. *Idem*, §526.
26. *Idem*, §525.
27. *Idem*, §652.
28. W P Keeton (ed) *Prosser and Keeton on the Law of Torts* 852, 5th edn, 1984.
29. Several states have enacted statutes that criminalize information theft. E.g., Ala. Code §13A-8–102(c)(1998); Ohio Rev. Code §2901.01 (West 1998); Va. Code §18.2–152.4(1)(Michie 1998); Wash. Rev. Code Ann. §9A.56.010 (West 1998).
30. 5 U.S.C. §552a.
31. 18 U.S.C. §1030.
32. *Idem*, §§2510 and 2520.

33. For a comprehensive discussion of information criminal and privacy protection law, see, generally, R T Nimmer *Information Law*, 8.01-.25 and 9.01–14.
34. 15 U.S.C. §1681.
35. 12 U.S.C. §§2601–2617.
36. See *idem*, the issuer must provide a method by which the user of the card could be identified as the person authorized to use it. Regulation Z of the Board of Governors of the Federal Reserve, 12 C.F.R. §226.13(d), provides that the identification may be made by signature, photograph, or fingerprint on the credit card or by electronic or mechanical confirmation.
37. A cardholder may authorize another person to use the card for a particular purpose; if the person uses it for other than that purpose, the *use* is nonetheless considered to be authorized under principles of agency law regarding apparent authority, even though the *purpose* was unauthorized. *See, e.g., Steiger* v *Chevy Chase Savings Bank*, 666 A.2d 479 (D.C. Ct. App. 1995); *Band* v *First Bankcard Center*, 644 So.2d 211 (La. Ct. App. 1994).
38. Kristof, *supra*, note 6, at C1.
39. The United States Sentencing Commission is an autonomous board within the federal judiciary charged with implementing sentencing practices and procedures in the federal system that will 'assure the ends of justice by promulgating detailed guidelines prescribing the appropriate sentences for offenders convicted of federal crimes' (US Sentencing Guidelines Manual Ch 1, Pt A, introductory comment (1998).
40. 28 U.S.C. §994(a) (authority for empowering the Sentencing Commission to issue sentencing guidelines.)
41. S.512 at §2.
42. See *idem*.
43. *See 18 U.S.C. §3663(a)(1)(B)(2) (Order of Restitution); see also 18 U.S.C. §3663A(a)(2).*
44. *Idem*.
45. S.512, 105th Cong. §3 (1998).
46. 'The United States Sentencing Commission shall consider ... any ... factor that [it] considers to be appropriate' in order to provide an 'appropriate remedy' for the crime of identity theft. *Idem*, §4.
47. *Idem*, at §2.
48. *Idem*, at §5.
49. *Idem*.
50. US Sentencing Guidelines Manual §2F1.1(b)(1)(1998).
51. See *idem*, §2F1.1(b)(2)(A).
52. See *idem*, §3B1.
53. See *idem*, §3A1.
54. See *idem*, §2F1.1(b)(2)(B).
55. In 1984, Congress established the nonpartisan body, consisting of seven voting members (three of which must be federal judges, and no more than four may be from the same political party). However, the Republicans and Democrats have not compromised on any of President Clinton's appointments. As of November 1998, all seven seats on the US Sentencing Commission were vacant. When Congress adjourned in October 1998, all but one Commissioner had resigned. See D A Shaw 'At Sentencing Commission, no one's home: thanks to politics, all seven seats are empty' *Los Angeles Daily Journal*, 18 November 1998, at 1.
56. The US Sentencing Commission has significant influence over the level of punishment that may be prescribed for any given crime. *Idem*.
57. *US Sentencing Guidelines Manual §§2B and 2F (1998).*
58. *S.512, at §5.*
59. *'Statement by the President on identity theft deterrence' The White House Publications*, 30 October 1998.

Cornell
Journal of Law
and Public Policy



Volume 8 Spring 1999 Number 3

DETERRING IDENTITY THEFT IN THE INFORMATION AGE: THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT

BRUCE ZUCKER
KURT SAUNDERS

COUNTERACTING IDENTITY FRAUD IN THE INFORMATION AGE: THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT

Kurt M. Saunders and Bruce Zucker†

identity, n; . . .2. *(a) the condition or fact of being some specific person. . .; individuality; (b) the condition of being the same as . . . someone assumed, described, or claimed.*[1]

ABSTRACT

The advent of the information age has created new challenges to the ability of individuals to protect the privacy and security of their personal information. One such challenge is that of identity theft, which has imposed countless hardships upon its victims. Perpetrators of this fraud use the identities of others to steal money, obtain loans, and generally violate the law. The Identity Theft and Assumption Deterrence Act of 1998, enforced by the Federal Trade Commission, makes the theft of personal information with the intent to commit an unlawful act a federal crime in the United States with penalties of up to twenty-five years imprisonment and a maximum fine of $250,000. This article first examines the problem of identity fraud and the inadequacy of existing remedies, and then assesses the need for and likely impact of the Act, as well as issues relating to the effectiveness of its future enforcement.

INTRODUCTION

With the emergence of the Internet and the increasing number of commercial transactions facilitated electronically, personal information is flowing throughout the country and around the world at speeds never before imagined. As a consequence, tax identification numbers, Social Security numbers, driver's license information, fingerprints, and similar private and confidential information are now more accessible than ever before.[2] An immense quantity of such information is often stored online

† The authors are Assistant Professors of Business Law at California State University, Northridge.

1 WEBSTER'S NEW TWENTIETH CENTURY DICTIONARY 902 (2d ed. 1983).

2 *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases*, 15 J.L. & COM. 395, 483-91 (1996).

in computer databases,[3] on proprietary networks of credit reference services,[4] and on the Internet.[5]

Described as the neoteric crime of the information technology era, identity theft is the illicit use of another individual's identifying facts (name, date of birth, Social Security number, address, telephone number, or other similar information) to perpetrate an economic fraud by opening a bank account, obtaining credit, applying for bank or department store cards, or leasing cars or apartments in the name of another.[6] How can such information be misused?

Consider the following scenario. Having impeccable credit, a person we will name Ida, decides to purchase a new car at a local car dealership. Intending to finance the purchase through credit arranged by the dealer, Ida completes a standard application form. After it conducts a credit check, the dealership denies her credit application. After further inquiry, Ida discovers that the credit reporting agency lists twenty-six open lines of revolving credit and three different car loans in her name. Further, the report lists eight different residences over the past year. Even though Ida believes that she has never made a delinquent payment, almost every one of her creditors reports her in default.

There is one problem—Ida never opened any of these credit lines herself. Someone stole her identity and used her perfect credit to obtain tens of thousands of dollars worth of goods and services. After exhausting her credit limit, these con-artists move on to the next unwitting victim, leaving Jane and her ruined credit in their wake.[7] What, if anything, can she do next?

---

3 The Department of Health and Human Services, the Selective Service System, and the Internal Revenue Service all cross-reference information using Social Security numbers. As a result, "anyone who knows an individual's SSN can amass a wealth of highly sensitive information about that individual." George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 526 (1990).

4 The three credit reporting agencies – Experian, Equifax, and Transamerica – store the credit information for countless numbers of consumers in their systems.

5 Indeed, the Internet is a veritable treasure trove of personal information where, starting with a person's name and address, one can find out, in a relatively short amount of time, "what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house and how much taxes you pay on it." Joshua Quittner, *Invasion of Privacy*, TIME, Aug. 25, 1997, at 33 (quoting Carole Lane, NAKED IN CYBERSPACE: HOW TO FIND PERSONAL INFORMATION ONLINE (1997)). *See also* The Stalker's Home Page: A Stalking We Go! (visited Feb. 21, 1999) http://www.glr.com/stalk.html (listing hyperlinks to web sites containing addresses, phone numbers, Social Security numbers, property taxes, and similar information).

6 Mark Grossman, *The Other You: The Misery of Identity Theft*, BROWARD DAILY BUS. REV., Sept. 4, 1998, at B1.

7 For other illustrations of hardships suffered by victims of identity theft, *see, e.g.*, Evan Hendricks ed., *Identity Theft Key to Major Medical Fraud Operation*, PRIVACY TIMES, Feb. 6, 1998, at 3-4; *Are You a Target for Identity Theft?*, CONSUMER REP., Sept. 1997, at 11; Brigid McMenamin, *Invasion of the Credit Snatchers*, FORBES, Aug. 26, 1996, at 257; *An Identity*

According to one major credit bureau, an estimated 480,000 people in the United States inquire into its fraud division annually.[8] Authorities estimate that identity theft imposes a cost on consumers approaching $100 million annually.[9] The United States Secret Service, which tracks major identity theft cases, reports that the dollar value of such cases has nearly doubled in the last year, and the Social Security Administration has seen a threefold increase in improper use of Social Security numbers.[10] According to credit reporting firms, fraud reports have climbed from less than 12,000 annually in 1992, to more than 500,000 currently.[11]

Using readily available technology, perpetrators of identity crimes typically break into computer databases containing personal identification information. Other times, they simply copy or modify fingerprints recorded or transmitted electronically.[12] In a prepared statement presented to Congress on this issue, the Federal Trade Commission illustrated other such means by which identity thieves carry out their schemes:

> Historically, identity thieves have accomplished their crimes through simple means—pickpocketing wallets, stealing pre-approved credit applications from mailboxes, or raiding trash dumpsters for discarded receipts and files. Recently, more sophisticated schemes are gaining popularity. One such method is securing low-level employment with a financial institution or other entity that gives the perpetrator access to consumer credit reports, or other identifying data, for their personal exploitation or for use by organized identity theft rings. For example, one fraud ring used such credit reports quickly to acquire fake I.D. cards, open "instant credit" accounts, and then run up thousands of dollars in debt. A recent case brought by the United States Secret Service demon-

---

Crisis: Credit-reporting Companies Need to Imporve Ways of Dealing with Consumer Claims of Fraud, Kathy Kristof, CHI. TRIB. (NORTH), Sept. 24, 1996, § 6, at 7; Robert Lemos, *Identity Theft a Big Business*, ZDNET NEWS, April 15, 1998, (visited Apr. 28, 1999) <http://www.zdnet.com/zdnn/content/zdnn/0414/306824.html>.

8 *Identity theft: How to Take Steps to Clear Your Name*, ORANGE COUNTY REG., August 23, 1998, at K4.

9 Grossman, *supra* note 6, at B1.

10 Kathy M. Kristof, *New Law to Assist Victims in Fight Against Identity Fraud*, LOS ANGELES TIMES, October 31, 1998, at C1, C3.

11 *Id.*

12 Theft and misuse of biometric identification data, including voice, retinal, and facial prints, are possible. *See, e.g.*, Robert Lemos, *Protecting Your Digital ID*, ZDNET NEWS, February 13, 1998 (visited Apr. 28, 1999) <www.zdnet.com/zdnn/content/zdnn/0213/285183.html>.

> strates how computer-savvy identity thieves may exploit information available over the Internet. In that case, the defendants were a Maryland couple who pled guilty in September 1997 to running up debt exceeding $100,000 under their stolen identities. They admitted to routinely using Internet databases to select their victims.[13]

This article examines the problems created by identity theft and explores recently enacted federal legislation intended to further proscribe it and offer assistance to its victims. Part I considers the nature and role of identity in society, including the inadequacy of existing statutory and common law to prohibit and redress identity theft. Part II discusses the material provisions of the Identity Theft and Assumption Deterrence Act of 1998, and assesses its probable effect on enforcement. Part III presents observations and comments of these authors as to the Act's likely impact on curtailing such crime and discusses some suggestions for effective enforcement.

THE IMPORTANCE OF IDENTITY IN SOCIETY AND ELECTRONIC COMMERCE, AND THE ROLE OF THE LAW IN ITS PROTECTION

A. IDENTITY, AUTHENTICATION, AND PRIVACY OF PERSONAL INFORMATION.

The notion of identity is inseparable from a person's intrinsic nature and sense of individuality. Among other things, it relates to a person's conscious sense of "self" and individuality, while also allowing others to recognize or distinguish him or her from others.[14] In society, the concept of identity is broader than merely knowing a person's name or recognizing a person's face. Rather, the identity of a person is often separate from his or her attributes and physical traits. In many instances, to learn or establish the identity of a person involves reference to some set of institutional or socially agreed upon identifying factors that authenticate a person's uniqueness in relation to others.

---

[13] *Prepared Statement of the Federal Trade Commission on "Identity Theft" Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Comm. on the Judiciary*, 105th Cong. 3 (1998) (statement of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission) [hereinafter *FTC Statement*]. *See also* Official Transcript of "FTC Consumer Identity Fraud Meeting," Aug. 20, 1996 at 11-13 (visited Feb. 21, 1999) <http://www.ftc.gov/ftc/conferences.htm>. The Federal Trade Commission maintains a privacy page at its web site to advise consumers how to protect personal information and how to obtain assistance in the event if they are victimized by identity theft. (visited Feb. 21, 1999) <http://www.ftc.gov/privacy/index.html>.

[14] For an extensive treatment of the concept of "identity" in its social and cultural context, see generally ERIK H. ERIKSON, IDENTITY AND THE LIFE CYCLE (1980).

Likewise, a person's identity, as well as the ability to prove it, is fundamental to many commercial and institutional transactions. For instance, businesses need to be assured that the person signing a contract or accepting delivery of goods is in fact who he says he is. Banks may require proof that the person who telephones to request information about her account or appears to make a withdrawal is in fact the same person who opened the account. In order to evidence identity, many institutions have resorted to systems that employ identifiers—such as Social Security or telephone numbers, mothers' maiden names, or birth dates—that are not necessarily unique or that may be easily discovered. They may issue identification devices—such as driver's licenses or membership cards—that may be readily stolen or duplicated. Sometimes, one institution or entity may use an identification document issued by another institution or entity as a means of establishing or authenticating a person's identity. This occurs, for example, when an airline or tavern requires production of a government issued photo identification.

Nevertheless, these apparently reliable solutions provide easy opportunities for corruption, fraud, and error.[15] These problems have been further exacerbated by the emergence of information technologies such as computerized databases and networks that can facilitate commercial and institutional transactions between parties separated by great distance or known to one another solely through the use of pseudonyms.[16] In such an environment, the opportunities for corruption, identity fraud, and error are substantially increased. Indeed, the emergence of the Internet as a potential new marketplace has underscored the need to establish secure and reliable means of identity authentication for electronic commerce. Presently used identity authentication procedures include passwords, data encryption systems, digital signatures, and firewalls, alone or in combination,[17] to ensure trust and confidentiality in the agreement formation process.[18]

---

[15] Virginia Ellis, *DMV Tries to Stem the Tide of Fake Licenses*, LOS ANGELES TIMES, Apr. 5, 1998, at A1, A26.

[16] Closely related to the issue of identity protection is the issue of whether anonymity in electronic communications should be legally guaranteed as a matter of free speech and privacy. *See* A. Michael Froomkin, *Anonymity and Its Enmities*, 1995 J. ONLINE L. 4 <http://www.law.cornell.edu/jol/froomkin.htm>.

[17] These security methods are discussed in Stimson Garfinkle & Gene Stafford, WEB SECURITY AND COMMERCE (1997).

[18] *See* Jane K. Winn, *Open Systems, Free Markets, and Regulation of Internet Commerce*, 72 TUL. L. REV. 1177, 1202 (1998); Matthew D. Ford, *Identity Authentication and 'E-Commerce,'* 3 J. INFO. L. & TECH. 1 (Oct. 30, 1998) <http://www.law.warwick.ac.uk/jilt/98-3/ford.html>; Anthony Ferraro, *Electronic Commerce: The Issues and Challenges to Creating Trust and a Positive Image in Consumer Sales on the World Wide Web*, FIRST MONDAY (1998) (visited Dec. 8, 1998) <http://www.firstmonday.dk/issues/issue3_6/ferrero/index.html>.

The unfortunate story of Terry Rogan, the plaintiff in *Rogan v. City of Los Angeles,*[19] illustrates how identity theft and inaccuracy of electronically stored information may turn into an ordeal. In 1981, McKandes, an escapee from an Alabama state prison, began using Rogan's name after he obtained a copy of Rogan's birth certificate in Michigan. McKandes then relocated to California and used Rogan's birth certificate to obtain a driver's license and other identification documents in Rogan's name. In early 1982, McKandes, who was still using Rogan's identity, was arrested by the Los Angeles Police Department (LAPD) on suspicion of murder, but was later released. Several months later, a California court issued an arrest warrant in the name of "Terry Dean Rogan," charging him with two robbery-murders which had occurred in Los Angeles. The police entered the warrant information into a national computer criminal information database known as the National Crime Information Center (NCIC), ensuring that every police officer in the United States would have access to, and could thereby become aware of, the outstanding warrant in the name of Terry Dean Rogan. Information containing McKandes' physical characteristics and fingerprints was added in June 1982.

In October 1982, Rogan was arrested by police on suspicion of trespass in Saginaw County, Michigan. The Michigan police discovered the robbery-murder warrant when they made an inquiry of the NCIC database. When the police compared Rogan's fingerprints and physical characteristics with those recorded in NCIC, they established that he was not the suspect wanted by the LAPD. Although the LAPD automatically removed the NCIC information after his October arrest, they reentered the same information containing Rogan's name in November 1982. In early 1983, county sheriff's deputies stopped Rogan's car in Saginaw, Michigan for failure to use a turn signal.

When the robbery-murder warrant information resurfaced during the routine computer check, the deputies ordered Rogan out of his car at gunpoint, searched, handcuffed, and took him into custody. While in jail, they handcuffed him to the metal bars of his cell while the police contacted the LAPD and the Saginaw police. The police released him two hours later once they clarified his true identity.

Later in 1983, police again stopped Rogan for a traffic offense and detained him due to the inaccurate NCIC information. The police later released Rogan. In July 1983, Rogan was driving from Michigan to Oklahoma to visit relatives when he was arrested by the Texas police. They released him only after they first stopped him, arrested him at gunpoint, handcuffed him based on the NCIC information and held him in

[19] 668 F. Supp. 1384 (C.D. Cal. 1987).

jail pending an investigation of his true identity. This process was repeated yet again in January 1984, in Saginaw, Michigan when a deputy sheriff stopped Rogan for driving without headlights. Finally, after that incident, the LAPD removed the NCIC record in Rogan's name.

Rogan brought suit against the City of Los Angeles under 42 U.S.C. § 1983 for deprivation of his constitutional rights due to a mistaken arrest.[20] The court held that the LAPD's use of the NCIC database was grossly negligent and awarded judgment to Rogan as a matter of law for the pain and humiliation suffered as a result of his experience.[21]

B. THE INADEQUACY OF EXISTING LAW AND THE NEED FOR NEW LEGISLATION

Common Law

Surprisingly, the legal system has not yet criminalized identity fraud. Under the federal criminal code, an individual who knowingly produces, uses, or traffics in false identification devices with the intent to defraud is subject to a maximum of twenty years in prison.[22] Assuming, however, that no false documents or identification devices are involved, nothing in the existing federal statutory scheme specifically prohibits a person from illegally *assuming* the identity of another individual with the intent to engage in fraudulent activity. Moreover, the United States Secret Service investigates and prosecutes only a small portion of these cases under the federal mail and wire fraud statutes.[23] Because many of these crimes involve such small amounts of money, they are too insignificant to justify use of limited investigative and prosecutorial resources.[24]

As the *Rogan*[25] case demonstrates, many identity thieves commit their frauds without ever obtaining a single identification document from the victim by simply appropriating information publicly available on Internet databases or elsewhere.

> [I]t's easy for the computer-literate among us to generate credit card numbers, because they are con-

---

20 *Id.* at 1386-87.

21 *Id.* at 1391. In another case of identity theft, the defendant searched through the desks of the victims to find social security numbers and other personal information and then fraudulently obtained credit cards. During the sentencing phase of the proceedings, two victims described how they faced arrest, were denied credit, and were forced to pay in cash and produce identification as a result of the defendant's fraud scheme. United States v. Wells, 101 F.3d 370, 372 (N.D. Tex. 1996).

22 18 U.S.C. § 1029 (1996).

23 *See* Kristof, *supra* note 10.

24 144 Cong. Rec. H9993, H9994 (daily ed. October 7, 1998) (statement of Rep. McCollum).

25 668 F.Supp. 1384 (C.D. Cal. 1987). *See also supra* text accompanying notes 3-5, and 8.

> structed by using a fixed mathematical procedure. Having generated, say, a hundred numbers, I can call a credit bureau and ask to verify a number. Having found a number in actual service – let's say yours – I could then call your bank, and giving your social security number (or address details, or mother's maiden name, or whatever else the bank uses to check identity), ask for a billing address change. Using the changed address, I could then charge purchases against your credit card, issue myself new credit cards or checkbooks and withdraw cash from your account.[26]

Once the thief garners the identifying information, documents are readily obtainable.[27]

Similarly, there appears to be no adequate civil remedy in tort because the common law does not recognize identity as a personal or property interest that should be protected from wrongful conduct.[28] Although tangible identification documents,[29] such as credit cards or driver's licenses, are personal property, they are merely indicia of their owner's identity. No court has ever classified an individual's identity as tangible personal property. The tort of fraud occurs when a defendant makes a misrepresentation of fact in order to induce another to act in reliance upon it,[30] but fraud is of no use to a victim of identity theft. A misrepresentation is fraudulent if the defendant knows or believes that the matter is not what he or she represents it to be.[31] The defendant is liable to the person who suffered a pecuniary loss by justifiably relying on the misrepresentation.[32] As such, under this theory, only the victim of the fraud itself, rather than the victim of identity theft, would have recourse against the defendant.

Invasion of privacy by the appropriation of name or likeness might also seem to offer relief. Invasion of privacy by appropriation of name or likeness occurs when the defendant appropriates the plaintiff's name or

---

26 GREGORY J.E. RAWLINGS, MOTHS TO THE FLAME: THE SEDUCTION OF COMPUTER TECHNOLOGY 10 (1996). *See also* Craig Bicknell, *Credit Card Fraud Bedevils Web*, WIRED NEWS (April 2, 1999) (visited Sept. 7, 1999) <www.wired.com/news/news/business/story/18904.html> (describing computer programs that generate credit card numbers that will pass an authorization check).

27 *Rogan*. 668 F.Supp. at 1387.

28 *See* RESTATEMENT (SECOND) OF TORTS § 224 Cmt.d (1965).

29 An identification document is made or issued by a government and, "when completed with information concerning a particular individual, is a type intended or commonly accepted for the purpose of identification of individuals." Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028(d)(2) (1999).

30 *See* RESTATEMENT (SECOND) OF TORTS § 525 (1977).

31 *See id.* § 526.

32 *See id.* §§ 525, 531.

image without consent for the defendant's own advantage.[33] This tort is not concerned with pirating the plaintiff's name *per se*, but with taking the plaintiff's name for the defendant's commercial advantage, such as "to advertise the defendant's product, or to accompany an article sold, to add luster to the name of a corporation, or for other business purposes."[34] Thus, a defendant is not liable unless he or she has used the plaintiff's name or likeness to imply the plaintiff's endorsement of the defendant's product or relationship to the defendant's business. Some courts have used this form of liability to recognize a right of publicity akin to a property right but have extended it only to celebrities and public figures.[35]

Federal Law

As to the protection of information itself, including data that may be used to establish or authenticate identity, existing law focuses upon concerns of security and privacy. Various federal statutes restrict the accumulation, storage, and distribution of information; other laws are designed to ensure that the information stored and distributed is accurate.[36] The Privacy Act, for example, regulates the maintenance and disclosure of personal data and personally identifiable information held by the federal government.[37] The Computer Fraud and Abuse Act imposes criminal penalties for the intentional and unauthorized access to government and federal interest computers for the purpose of altering, damaging, or destroying information.[38] Under the Electronic Communications Privacy Act, sanctions are imposed for unauthorized interception or disclosure of, as well as unauthorized access to, electronic communications stored in a facility involved in electronic communications services and for knowingly divulging the content of such communications while in storage.[39] While these laws have aided in limiting the threat of a dramatic decrease in privacy and an inevitable increase in losses due to inaccurate information, they provide little or no relief for the victims of identity theft and misuse.[40]

---

33 *See id.* §§ 652A, 652C.

34 W. PAGE KEETON, ET ALL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 852 (5th ed. 1984). In addition, the piracy for other purposes such as, "impersonation to obtain credit or secret information, or by posing as the plaintiff's wife of providing a father for a child on a birth certificate" also constitutes invasion of privacy. *Id.*

35 *See e.g.* White v. Samsung Elec. Am., Inc., 971 F.2d 1395, 1397-1400 (9th Cir. 1992).

36 Several states have enacted statutes that criminalize information theft. *E.g.*, ALA. CODE § 13A-8-102(c) (1994); OHIO REV. CODE § 2901.01 (10)(a), (3)(j) (Anderson 1999); VA. CODE ANN. § 18.2-152.4(1)(3) (Michie 1998); WASH. REV. CODE § 9A.56.010(5) (West 1999).

37 5 U.S.C. § 552a (1995).

38 18 U.S.C. § 1030 (1995).

39 *Id.* §§ 2510, 2511 (1995).

40 For a comprehensive discussion of information criminal and privacy protection law, see generally RAYMOND T. NIMMER, INFORMATION LAW ¶¶ 8.01-.25 & 9.01-14 (1996).

In addition, federal consumer credit protection statutes provide limited assistance to victims of identity fraud. For instance, the Fair Credit Reporting Act regulates the collection and use of personal data by credit reporting agencies by prohibiting disclosure of consumer credit reports without consent, unless such disclosure is made for a legitimate business reason.[41] The Truth-in-Lending Act, enacted in 1968, is primarily a disclosure law that requires sellers and lenders to fully disclose credit or loan terms to debtors.[42] One amendment to the Truth-in-Lending Act, known as the Fair Credit Billing Act, limits the liability of credit cardholders to $50 per card for unauthorized charges made before the credit card issuer is notified that the card has been lost or stolen.[43] The use of a credit card is unauthorized only when it is used without the permission or approval of the cardholder.[44]

These various statutes have been ineffective in deterring identity theft and providing relief to victims for several reasons. The laws have been ineffective because their approach to the problems that result from identity fraud is scatter-shot, with multiple statutes and government agencies having jurisdiction over this misconduct. More importantly, Congress enacted these laws with other purposes in mind, such as information privacy or accuracy, and the statutory definitional language is often too narrow to apply to identity theft. In addition, the statutes were intended to protect financial institutions and therefore recognize creditors as the victims, rather than the consumers.[45] As will be discussed in the next section, the Identity Theft and Assumption Deterrence Act[46] specifically defines identity theft as a crime, recognizes the consumer as the victim, and provides for specific remedies and penalties.

THE IDENTITY THEFT AND ASSUMPTION DETERRENCE ACT

In 1997, Senator Jon Kyl (R-Arizona) introduced Senate Bill 512, known commonly as the Identity Theft and Assumption Deterrence Act.

---

41 15 U.S.C. § 1681 (1995).

42 15 U.S.C. § 1601 (1995).

43 *Id.* § 1643. The issuer must provide a method by which the user of the card could be identified as the person authorized to use it. Regulation Z of the Board of Governors of the Federal Reserve, 12 C.F.R. § 226.12(b)(2)(iii) (1999), provides that the identification may be made by signature, photograph, or fingerprint on the credit card or by electronic or mechanical confirmation.

44 A cardholder may authorize another person to use the card for a particular purpose; if the person uses it for other than that purpose, the *use* is nonetheless considered to be authorized under principles of agency law regarding apparent authority, even though the *purpose* was unauthorized. *See* Stieger v. Chevy Chase Savings Bank, 666 A.2d 479, 482-3 (D.C. 1995); Band v. First Bankcard Center, 644 So.2d 211, 217 (La. Ct. App. 1994).

45 *See FTC Statement*, *supra* note 13, at 11-13.

46 Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. § 1028 (1999)).

Congress passed the bill in October 1998 and it went into effect in January 1999.[47] The Act intents to expressly criminalize identity theft, and classify private citizens as direct victims of such conduct.[48] In addition, the Act directs the United States Sentencing Commission to incorporate the crime of identity theft into the appropriate sections of the United States Sentencing Guidelines Manual and to select the appropriate corporal and financial sanction for federal judges to use at sentencing.[49]

The Act amends Title 18 of the United State Code to specifically criminalize identity theft.[50] As enacted, 18 U.S.C. § 1028(a)(7) (Fraud and Related Activity in Connection with Identification Documents and Information) will add the following pertinent language:

[Whoever] 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, [commits identity theft].[51]

The Act defines "means of identification" as any name or number that may be used to identify a specific individual.[52] The penalties for violations of this section include fines, supervised release, and anywhere from one to 25 years in custody.[53]

Under current law, federal courts are precluded from awarding restitution to individuals who incur expenses associated with the theft of their identities. If, for example, an individual spent several thousand dollars in attorney fees in order to correct his credit history, to deal with various

---

47 *Id.* A parallel bill was introduced into the House of Representatives as H.R. 4151, which became the final version of the bill that President William Jefferson Clinton signed into law on October 30, 1998. *See* Statement by President William J. Clinton Upon Signing H.R. 4151, 5 U.S.C.C.A.N. 703 (October 30, 1998).

48 Identity Theft and Assumption Deterrence Act of 1998, § 3(a), (d), 18 U.S.C. § 1028(a), (d)(3) (1999).

49 Identity Theft and Assumption Deterrence Act of 1998, § 4, 28 U.S.C. § 994 note (1999). The United States Sentencing Commission is an autonomous board within the federal judiciary charged with implementing sentencing practices and procedures in the federal system that will "assure the ends of justice by promulgating detailed guidelines prescribing the appropriate sentences for offenders convicted of federal crimes." 28 U.S.C. § 994(a)(1) (1995) (authority for empowering the Sentencing Commission to issue sentencing guidelines). *See also* U.S. SENTENCING GUIDELINES MANUAL § 1A(1) (1998).

50 *See* Statement by President William J. Clinton Upon Signing H.R. 4151, 5 U.S.C.C.A.N. 703 (October 30, 1998).

51 18 U.S.C. § 1028(a)(7) (1999).

52 *Id.* § 1028(d)(3).

53 *Id.* § 1028(b). The severity of the penalties depend on the specifics of the crime. For example, if the offense involved, "the transfer or use of one or more means of identifications" and provided that stay perpetrator "obtains anything of value" amounting to at least $1,000 within any one period, the statutory minimum is 15 years imprisonment. *Id.* § 1028 (b)(1)(D). If the identity theft offense involved such conduct as drug trafficking, a crime of violence, or international terrorism, the statutory maximum may range anywhere from one year to 25 years in custody. *Id.* § 1028(b)(3), (b)(4).

creditors affected by the identity theft, or to clear his reputation, federal courts could not award restitution of these expenses because this individual would not be considered a "victim. . .directly and proximately harmed. . . ."[54] Only direct victims of the fraudulent activity (such as banks, merchants, or other such entities ultimately responsible for rectifying the damage) could receive awards of restitution.[55] Although the Senate version of the Act allowed for restitution to consumer victims, the House version of the Act did not include such restitution.[56]

Additionally, the Act instructs the United States Sentencing Commission to amend the United States Sentencing Guidelines to include the concept of "identity theft" into the relevant fraud-related guideline sections.[57] The Act gives the Sentencing Commission broad discretion in how to carry out this mandate,[58] but does order it to consider, *inter alia*, the extent to which the number of victims were involved in the offense, the harm to a victim's reputation, a victim's inconvenience and other difficulties resulting from the offense, the number of identification documents used by the perpetrator, and the extent to which the value of the loss to any individual caused by the offense is somehow an inadequate measure of appropriate penalty.[59]

A perfect illustration of the need for harsher punishment for identity theft under the guidelines than is currently in place under existing law is found in the case of *United States v. Wells*.[60] In *Wells*, the government charged the offender with illegally acquiring personal information and social security numbers of at least two individuals.[61] She used this information to obtain credit cards in the names of those individuals and committed the fraud accordingly.[62]

Wells pleaded guilty to one count of mail fraud.[63] The district court sentenced her to a 30-month term of imprisonment.[64] In order to arrive at the 30-month term, the district court elected to depart upward from the sentencing guideline range.[65] In exercising its discretion to depart,[66] the

---

54 *See* 18 U.S.C. § 3663(a)(2) (1998). *See also* 18 U.S.C. §3663A(a)(2)(1999).

55 18 U.S.C. § 3663(a)(2) (1998).

56 *Compare* S. 512, 105th Cong. § 3 (1998) *with* H.R. 4151, 105th Cong. (1998).

57 28 U.S.C. §994 note (1999).

58 "The United States Sentencing Commission shall consider. . .any. . .factor that [it] considers to be appropriate" in order to provide an "appropriate remedy" for the crime of identity theft. *Id.*

59 *Id.*

60 101 F.3d 270 (5th Cir. 1996).

61 *Id.* at 371.

62 *Id.*

63 18 U.S.C. § 1341 (1996).

64 *Wells*, 101 F.3d at 371.

65 *Id.*

66 The district court is bound to follow the United States Sentencing Guidelines when imposing a sentence. However, it may depart from the guideline sentencing range whenever

court considered the fact that individuals "whose identity Wells assumed lost days from work, feared arrest, were forced to appear in court, struggled to repair their credit rating, were not able to use the credit cards in their possession, and still face problems connected with this offense."[67]

The court in *Wells* observed that the Sentencing Guidelines did not adequately take into account the "extreme personal victimization" that the identity crimes can inflict upon their victims such that the court found it necessary to take the unusual and rare step of departing from the range of guidelines for imprisonment.[68]

The last portion of the Act directs the Federal Trade Commission (FTC) to establish a centralized clearinghouse to record and track complaints, and to provide consumer education service for victims of identity theft.[69] Finally, the Act instructs the FTC to implement procedures for referring complaints to the three major national consumer-reporting agencies (Experian/TRW, TransUnion, and Equifax) and to channel them to the respective law enforcement agencies for investigation.[70]

THE IMPACT OF THE ACT

The Identity Theft and Assumption Act accomplishes two main objectives. First, the Act provides for stiff penalties for perpetrators of this crime[71] and implements certain procedures for investigation and enforcement.[72] Second, it directs the Federal Trade Commission ("FTC") to establish procedures for educating the public, receiving complaints, and coordinating enforcement efforts with various investigatory agencies.[73]

Regarding the first objective, the Sentencing Commission may choose to enact harsh penalties for such conduct. Under the current system, perpetrators of fraud receive sentencing enhancements in direct correlation with the amount of loss caused by their activities,[74] the amount of planning involved,[75] if a jointly undertaken activity, the level of so-

---

the court finds that, "there exists an aggravating or mitigating circumstances of a kind, or to a degree, not adequately taken into consideration by the Sentencing Commission in formulating the guidelines that should result in a sentence different from that described." U.S. SENTENCING GUIDELINES MANUAL § 1A (4)(b) (1998); U.S. SENTENCING GUIDELINES MANUAL § 5K2.0 (1998); 18 U.S.C. § 3553(a) (1999); Koon v. United States, 518 U.S. 81, 92 (1996).

67 *Wells*, 101 F.3d at 374.

68 *Id.*

69 Identity Theft and Assumption Deterrence Act of 1998, § 5, 18 U.S.C. §1028 note (1999).

70 *Id.*

71 18 U.S.C. § 1028 (1999).

72 *Id.*

73 *Id.* at note.

74 U.S. SENTENCING GUIDELINES MANUAL § 2F1.1(b)(1) (1998).

75 *Id.* § 2F1.1(b)(2)(A).

phistication of the role the perpetrator played,[76] the susceptibility and status of the victims,[77] and the number of victims involved in the offense.[78] Depending upon the composition of the Sentencing Commission,[79] it could enact a relatively harsh guideline for the imposition of punishment for offenders of identity theft.[80] Considering the unique nature and consequences of identity theft, the Commission could establish a guideline section that is distinct from Part B (Offenses Involving Property) and Part F (Offenses Involving Fraud or Deceit) of the U.S. Sentencing Guidelines Manual, rather than incorporate it into one of the existing guideline sections.[81] This would ensure satisfactory consideration of the various factors detailed in the Act.

As to the second objective, the Act makes clear that the FTC is the primary agency responsible for its implementation and coordination of enforcement. Congress directed the FTC to educate the public on identity theft, receive and document reports of such illicit conduct, coordinate any complaints by consumers of identity theft with law enforcement, and establish procedures for the public to file complaints.[82] The Act gives the FTC one year to accomplish these three primary tasks. However, nothing in the Act provides for a periodic assessment of the success of implementation or for the FTC to report to Congress whether it is in compliance with these directives. There appears to be a need for such assessment procedure.

Although the Identity Theft and Assumption Deterrence Act specifically recognizes identity theft as a distinct crime of its own, identifies individual consumers as victims separate and apart from institutional victims, and provides for specific penalties and remedies, it remains unclear as to whether it will have any tangible or measurable effect on deterrence, punishment, or providing any new remedies to its victims.

---

76 *Id.* § 3B1.1.

77 *Id.* § 3A1.1(b)(1).

78 *Id.* § 2F1.1(b)(2)(B).

79 In 1984, Congress established the nonpartisan body, consisting of seven voting members (three of which must be federal judges, and no more than four may be from the same political party.) However, the Republicans and Democrats have not compromised on any of President Clinton's appointments. When Congress adjourned in October 1998, all but one Commissioner had resigned. As of November 1998, all seven seats on the U.S. Sentencing Commission were vacant. *See* Daniel A. Shaw, *At Sentencing Commission, No One's Home: Thanks to Politics, All Seven Seats are Empty*, LOS ANGELES DAILY JOURNAL, November 18, 1998, at 1.

80 The United States Sentencing Commission has significant influence over the level of punishment that may be prescribed for any given crime. *Id.*

81 U.S SENTENCING GUIDELINES MANUAL §§ 2B, 2F (1998).

82 18 U.S.C. § 1028 note (1999).

CONCLUSION

With the onset of the information age, the fundamental ability to protect one's personal information and identity is now more in jeopardy than ever. The widespread use of computer databases and the Internet to store and transmit information have made identity theft even easier to perpetrate. Indeed, empirical studies indicate that the number of crimes related to identity theft is steadily increasing, with enormous cost to the victims. Surprisingly, only a handful of states have acted to proscribe this misconduct, which often involves interstate commerce, and identity theft had not been specifically banned by federal legislation until the present time. However, the enactment of the Identity Theft and Assumption Deterrence Act of 1998 specifically criminalizes identity fraud and empowers the federal courts to award consequential damages to victims of such crimes.

When President Clinton signed the Act into law, he said, "as we enter the Information Age, it is critical that our newest technologies support our oldest values."[83] Implementation of this act will further empower law enforcement, consumer protection agencies, and the public to combat identity thieves and deter such conduct as society continues to see the expansion of advanced technology.

[83] *See* Statement by President William J. Clinton Upon Signing H.R. 4151, 5 U.S.C.C.A.N. 703 (October 30, 1998).