BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

Counteracting Online Identity Fraud under the Identity Theft and Assumption Deterrence Act

Kurt M. Saunders & Bruce Zucker
Assistant Professors of Business Law
California State University, Northridge

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.*

ABSTRACT

The information age has created new challenges for individuals in protecting the privacy and security of personal information, including that of identity theft. Perpetrators of this fraud misappropriate the identities of others to steal money, obtain loans, and otherwise violate the law. The Identity Theft and Assumption Deterrence Act 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 fifteen years imprisonment and a maximum fine of $250,000. This paper examines the problem of identity fraud and the inadequacy of existing remedies, and then assesses the need for and related issues of enforcement of the Act.

With the emergence and expansion of the Internet and the number of commercial transactions facilitated electronically, personal information such as tax identification numbers, Social Security and social insurance numbers, driver's license information, fingerprints, and similar private and confidential information are now more accessible than ever before. Much of this information is stored in computer databases, on proprietary networks of credit reference services, and available on the World Wide Web. Unfortunately, such information can also be easily misused.

Consider this very possible scenario: An individual with an impeccable credit history decides to purchase a new car at a local car dealership. Intending to finance the purchase through credit arranged by the dealer, she completes a standard credit application. After the dealer conducts a credit history check, she is told that her credit application has been denied. After further inquiry, she finds out that the credit reporting agency lists her as holding twenty-six open lines of revolving credit and three different car loans. She also discovers that it lists eight different residences over the past year. Even though she has never made a delinquent payment, almost every one of her creditors has reported her in default. Moreover, she never opened any of these credit lines herself. Someone obviously stole her identity and used her impeccable credit to obtain tens of thousands of dollars worth of goods and services. After exhausting her credit limit, this identity thief moved on to the next unwitting victim, leaving this individual and her ruined credit behind. What, if anything, can she do about this situation?

This individual has become a victim of what has been described as the neoteric crime of the information technology era -- identity theft, or the illicit utilization of another individual's identifying facts (name, birthdate, Social Security number, address, telephone number, and 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. An estimated 40,000 people in the United States fall victim to such crimes each year and authorities estimate that identity theft imposes a cost on consumers of almost $100 million annually. The United States Secret Service, which tracks major identification theft cases, has reported that the dollar value of such cases has nearly doubled in the last year, and the Social Security Administration has witnessed a threefold increase in improper use of Social Security numbers. According to several credit reporting firms, identity fraud reports have increased from less than 12,000 annually in 1992 to more than 500,000 presently.

Using readily available technology, perpetrators of identity crimes typically break into computer databases containing personal identification information. In a prepared statement presented to the U.S. Congress on this issue, the Federal Trade Commission described how other identity thieves can perpetrate this fraud:

> 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 September1997 to running up debt exceeding $100,000 under their stolen identities. They admitted to routinely using Internet databases to select their victims.

In this paper, we examine the problems created by identity theft and explore a new federal law intended to proscribe it and offer assistance to its victims. We consider the importance of identity in commercial transactions and the inadequacy of existing statutory and common law to prohibit and redress identity theft. We then discusse the material provisions of the Identity Theft and Assumption Deterrence Act. Finally, we present our observations and comments as to its likely impact on preventing this crime and suggest approaches for its effective enforcement.

I. The Role of Identity in Electronic Commercial Transactions and the Inadequacy of Existing Law

A person’s identity, and his ability to prove it, is central to most commercial transactions. Merchants need to be assured that whoever signs a particular contract or accepts delivery of certain goods is, in fact, who she represents herself to be. Likewise, banks typically require proof of identity when a customer makes a telephone inquiry or a withdrawal of funds from an account. In order to establish identity, commercial institutions often resort to systems that employ various identifiers -- such as Social Security or telephone numbers, mothers’ maiden names, or birth dates -- that are not necessarily unique or that could be easily discovered. Sometimes, they issue identification or access devices -- such as driver’s licenses, ATM cards, credit cards, or membership cards -- that may be easily duplicated or stolen. On occasion, one entity borrows the identifier issued by another entity as a means of establishing or authenticating a person’s identity. This may occur, for instance, when an airline or tavern requires production of a government issued photo identification.

Unfortunately, these apparently reliable verification devices provide easy opportunities for corruption, fraud, and error. In the electronic setting, the opportunities for identity theft are substantially increased. The advent of the Internet has underscored the need to establish secure and reliable channels of electronic commerce for identity authentication. Presently used processes for

verification of identity use passwords, data encryption systems, digital signatures, steganography, or digital certificates, or combinations of these, to ensure trust and confidentiality in the contract formation process.

It is somewhat surprising that the American legal system would not have already criminalized identity theft. Under federal law, anyone who obtains, uses, or transfers false identification for the purpose of committing a fraudulent act without the consent of the holder of the identification commits a felony. However, no federal statute specifically prohibits a person from illegally assuming the identity of another individual unless false documentation is involved in the activity. In fact, many of identity thefts occur without the perpetrator ever obtaining even a single identification document, given that the fraud may often result solely from identifying information found in publicly available databases.

As to the protection of the information itself, including data that may be used to establish or authenticate identity, existing federal law is concerned only with issues of security and privacy. Several federal statutes restrict the accumulation, storage, and distribution of information, while other laws ensure that the information stored and distributed is accurate. The Privacy Act, for instance, regulates the maintenance and disclosure of personal data and personally identifiable information held by the federal government. The Computer Fraud and Abuse Act makes illegal the intentional and unauthorized access to government and federal interest computers for the purpose of altering, damaging, or destroying information. Under the Electronic Communications Privacy Act (ECPA), criminal sanctions are imposed for unauthorized interception or disclosure of, or unauthorized access to, electronic communications stored in a facility involved with electronic communications services. The ECPA also prohibits knowingly divulging the content of such communications while in storage. While all of these laws have limited somewhat the threat of identity theft, they afford little or no relief for victims of this misconduct.

Federal consumer credit protection statutes also provide little or no assistance to victims of identity fraud. For example, the Fair Credit Reporting Act regulates the collection and use of personal data by credit reporting agencies in that it prohibits disclosure of consumer credit reports without the consent of the consumer unless the person or entity seeking the information needs it for a "legitimate business reason." The Truth-in-Lending Act requires lenders and merchants to fully disclose credit or loan terms to their customers, whereas the Fair Credit Billing Act limits the liability of credit card holders to $50 per card for any unauthorized charges made before the credit card issuer is notified that the card has been lost or stolen.

II. The Scope of the Identity Theft and Assumption Deterrence Act

The Identity Theft and Assumption Deterrence was signed into law by President Clinton on October 30, 1998. The Act is intended to expressly criminalize identity theft, classify private citizens as direct victims of such conduct, and allow courts to include losses incurred by individual consumers into restitution orders for expenses resulting from rectifying their credit records. Under amended section 1028(a) of the United States Code:

> 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].

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

Under existing law, federal courts are precluded from awarding restitution to individuals who incur expenses associated with the theft of their identities. For example, if 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 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]." 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.

Consequently, the Act amended 18 U.S.C. § 3663A so as to *mandate* that the federal courts order restitution for consumer victims. As defined by 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."

Additionally, the Act instructs the United States Sentencing Commission to amend the United States Sentencing Guidelines to include the "identity theft" in the relevant fraud-related guideline sections. The Act gives the Sentencing Commission broad discretion carrying out this mandate, but does order it to consider 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 central clearinghouse to record and track complaints and to provide consumer education service for victims of identity theft. The FTC is directed to implement procedures for referring complaints to the three major national consumer-reporting agencies and to forward them to the appropriate law enforcement agencies for further investigation.

III. The Enforcement and Likely Impact of the Act

The Identity Theft and Assumption Act accomplishes three principal 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 designing restitution orders. Second, the Act provides for more severe penalties against perpetrators of this crime and implements certain procedures for investigation and enforcement. 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.

As to the first objective, victims will have enforceable restitution orders with which to attempt to obtain reimbursement. However, like many judgments entered against defendants who are involved in such activities, such individuals are often judgment proof, without assets or income. Thus, the chance of these victims actually receiving any compensation from the restitution orders may be negligible.

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, the amount of planning involved, if a jointly undertaken activity, the level of sophistication of the role the perpetrator played, the susceptibility and status of the victims, and the number of victims involved in the offense.

Depending upon the composition of the Sentencing Commission, it could enact a relatively harsh guideline for the imposition of punishment for offenders of identity theft. 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.

With respect to the third objective, the Act makes clear that the FTC is the primary agency responsible for its implementation and coordination of enforcement. Congress instructed 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. The Act gives the FTC one (1) year to accomplish these three responsibilities. However, nothing in the Act provides for assessment of the success of implementation or for the FTC to report to Congress whether it is in compliance with these directives.

IV. Conclusion

The ability to protect one's personal information and identity is in greater jeopardy than ever in the electronic age. When President Clinton signed the Identity Theft and Assumption Deterrence Act into law, he remarked: "[A]s we enter the information age, it is critical that our newest technologies support our oldest values." Implementation of this Act will empower law enforcement, consumer protection agencies, and the public to combat identity thieves and deter such conduct made more easily perpetrated by the advent of the information age.