

## World Internet Law Report

International Information for International Businesses

Monthly news and analysis on Internet law and regulation from around the world

Volume 5, Number 8

August 2004

## Privacy

### Identity Theft in the United States

*By Holly K Towle, a Partner in the Seattle office of Preston Gates & Ellis LLP and chair of the firm's E-Commercial Law practice group. The author may be contacted at [hollyt@prestongates.com](mailto:hollyt@prestongates.com)*

For centuries, philosophers have considered the concept of human identity, a notion that refers to an individual's sense of "self" and distinguishes one individual from another. In modern society, not only does one's identity – and the ability to prove it – serve to distinguish one person from another, but it also plays an obvious role in many of today's commercial and personal transactions.

In one sense there is nothing new here given that determining with whom one is really dealing has always been important.<sup>1</sup> However, making that determination becomes more complex when e-commerce is involved because there is no face-to-face interaction and a driver's license picture or handwritten signature cannot be easily examined (even assuming they are valid). Data can be collected that tends to identify a person, but laws may restrict that collection and some identifiers may be public information or discoverable with an ease that may make the information of questionable use. This situation provides opportunity for illegal activity which can be exacerbated in electronic settings.

But the reality is that this opportunity has always existed and that "offline" methods for illegal activities cannot be ignored. For example, a 2003 survey by the United States Federal Trade Commission (FTC) indicated that *a lost or stolen wallet or pocket book, or theft of the victim's postal mail (including lost or stolen credit cards, checkbooks, and social security cards)*, was the most commonly mentioned way that an identity thief obtained information.<sup>2</sup> A study by Michigan State University study to be published later this year, echoes or expands this by apparently finding that as many as 70 percent of all identity-theft cases originate with information stolen in a workplace, rather than through hacker intrusions, home robberies or mail fraud.<sup>3</sup> Identity thieves also include persons who give the name of another person in order to delay or avoid being charged with a crime, and there is nothing more "face-to-face" or "non-electronic" than an arrest.

The likely difference between now and yesterday is not a difference between online and offline activities, but changes in technology generally which allow thieves to do more, online or offline:

At one time, not that many years ago, a breeder document, such as a driver's license, meant something; it could be used to establish a person's identity with little or no question. Now, technology has enabled criminals to produce fraudulent documents, which can be used to procure additional fraudulent documents. Counterfeit documents, such as credit cards, used to be easily detectable; now it is relatively easy to produce a counterfeit hologram that usually passes for the real thing. . . . Technology and the ability of the criminal element to adapt and defeat existing identification



methodologies, predicated on breeder documents that are susceptible to counterfeiting, have made it necessary to develop different, more advanced identity authentication systems.<sup>4</sup>

Whether real or hyperbole, identity theft is being tied to the information age and has been described as “the crime of the new millennium”.<sup>5</sup> While certainly this potential exists, the FTC’s 2003 study actually indicates that all forms of identity theft have impacted only 4.6 percent of the U.S. population.<sup>6</sup> While no one would want to be in any group of identity theft victims, the point is that media coverage tends to leave the impression that this is an urgent, major crime for a hugely significant portion of the American public, and legislators are scrambling to get on the bandwagon with ever increasing amounts of legislation. Hence the need to look at this topic in more detail, including from a legal perspective.

## What Is Identity Theft?

“Identity theft” is a term referring to a variety of crimes, all of which involve “stealing” someone’s personal identifying information. The identity thief may use a variety of methods to obtain this information, ranging from “basic street theft” to “sophisticated, organized crime schemes involving the use of computerised databases or the bribing of employees with access to personal information on customer or personnel records”.<sup>7</sup> Once the thief obtains the necessary information, he can transact business posing as his victim. In a recent Internet twist, two identity thieves opened accounts to sell goods on an Internet auction site – but there were no goods and they had opened their accounts under the names of their victims. When buyers at the auction did not receive their goods, they thought the victims, not the thieves, were the sellers who had defrauded them.<sup>8</sup>

What does identity theft typically involve? As explained by one group:

The term, “identity theft,” is itself complicated because it is used to refer to several different types of crimes in which personal or financial data is compromised. However, as the number of cases have increased, patterns have emerged, making it possible to classify identity theft into the following categories:

- Fraudulent Authentication/One-Time Identity Theft
- Financial Institution Fraud
- Credit Card Fraud
- Fraudulent Loans
- Communications and Utilities Fraud
- Other.<sup>9</sup>

An identity thief’s fraudulent activities generally take one (or both) of two basic forms: so-called “criminal identity theft” (providing a victim’s personal identifying information to law enforcement upon arrest) or financial fraud, further distinguished as “true name fraud” (using a victim’s identifying information to open new accounts in the victim’s name) and “account takeover” (gaining access to a victim’s existing accounts and making fraudulent charges). Although criminal identity theft does take place, traditionally the vast majority of identity thefts in the United States have been financially related<sup>10</sup> and are usually a component of one or more other white-collar or financial crimes. However, there is also “identity fraud,” which encompasses identity theft but also includes

creating or using a *fictitious* identity, as opposed to stealing and using a real one.<sup>11</sup> In modern society, it may be that we will actually see as much or more of that kind of criminal activity than the type to which regulators tend to be responding most:

The use of a false identity created from fraudulent documents or a stolen identity (identity theft) in the commission of a crime has long been used by criminals and criminal organizations to facilitate criminal activities and avoid detection. As is evident from the previous section, quantifying the impact of identity fraud is difficult, but as the statistics in the next sections report, terrorism, money laundering and financial crimes, drug trafficking, alien smuggling, and weapons smuggling are growing concerns for the public and private sectors. Laws and regulations that have been instituted since 1998 are another indicator of the dramatic increase in the widespread use of these methods by criminals and terrorists.<sup>12</sup>

## How Does Identity Theft Happen?

An endless list of scams provides an opportunity for identity theft. Many of them are listed at a site maintained by the Identity Theft Resource Center.<sup>13</sup> But even ordinary activities provide opportunity for identity theft: lost or stolen items such as postal mail, wallets, purses, checkbooks, and cards (social security or credit cards) are common causes. A catalogue of additional methods can be found in a paper prepared by the National Automated Clearing House Association.<sup>14</sup>

## Who is an Identity Thief?

According to the FTC’s 2003 Report, if the victim knows the thief then the crime is usually more serious – 26 percent of all victims knew the thief’s identity,<sup>14</sup> which tended to be as follows:

- In 35 percent of the cases where the victims know (nine percent of all victims), the thief is a *family member or relative*.<sup>16</sup>
- In 23 percent of the cases (six percent of all victims), the thief was someone who worked at a *company or financial institution* that had access to a victim’s personal information.<sup>17</sup>
- In 18 percent of the cases (five percent of all victims) the thief was a *friend, neighbor, or in-home employee*.<sup>18</sup>
- In 16 percent of the cases (four percent of all victims), the thief was a *stranger* but the victim later became aware of the identity.

The above statistics are interesting because some media coverage leaves one with the impression that identity theft is committed by faceless strangers. To the contrary, that is the lowest category of known thieves. Of course, the above accounts for only nine percent of all victims so, obviously, most victims do not know who the thief was and, thus, a range of additional possibilities exists. It may be that in this large group lies the stranger-thieves of the policy debate.

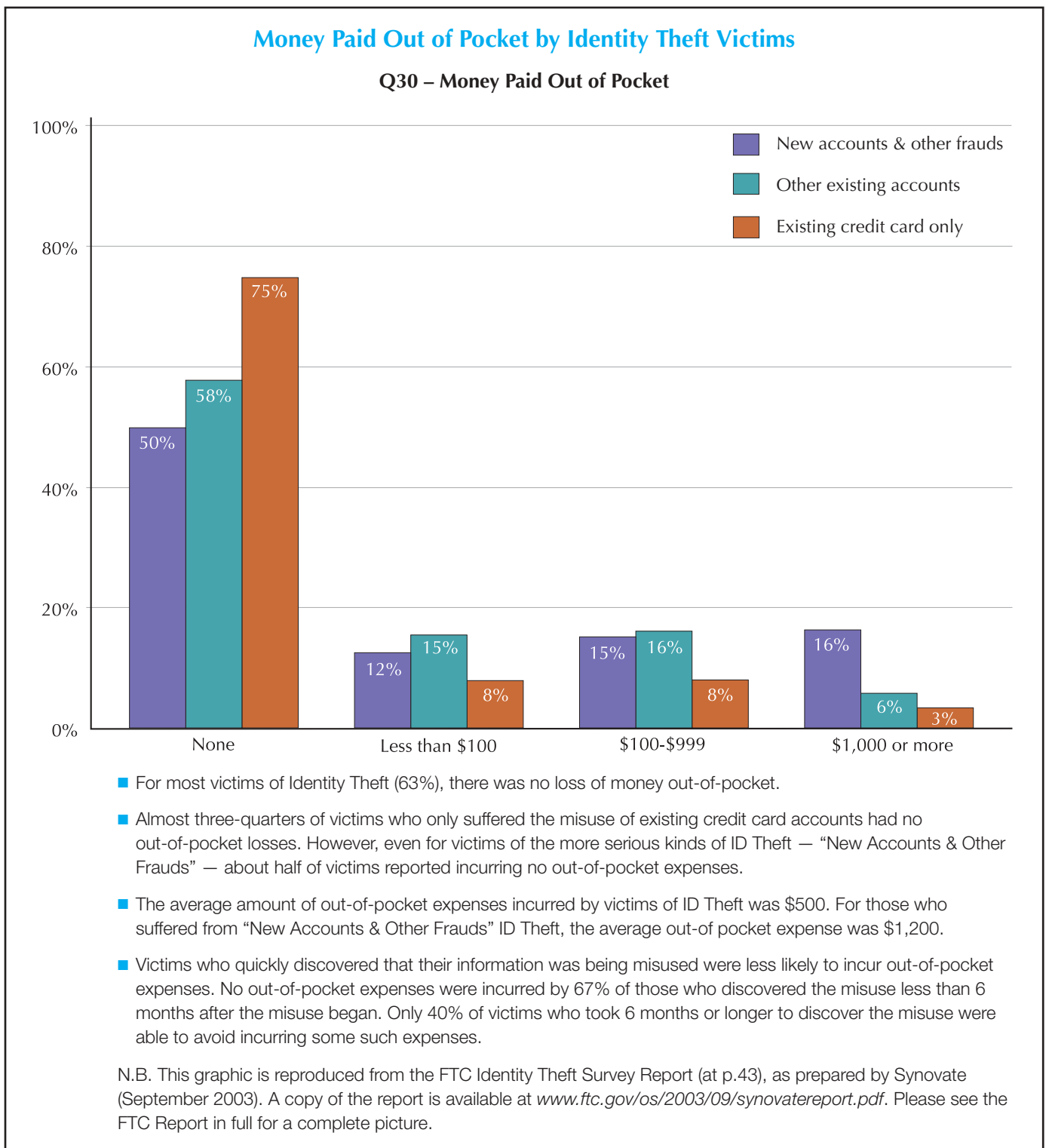
## Responses to Identity Theft

Interestingly, the FTC 2003 Report indicates that for most victims of identity theft (63 percent), there is no loss of money out-of-pocket;<sup>19</sup> 35 percent of all victims were able to resolve all problems in one hour or less;<sup>20</sup> and regardless of the misuse the

victim encountered, over half of those surveyed said they were “not very” or “not at all” concerned that it might happen to them again.<sup>21</sup> This may result from the fact that the most common instances of theft pertain to existing credit card accounts, and victims were “overwhelmingly” satisfied with the credit card issuer’s response to the victim’s report of misuse.<sup>22</sup> Satisfaction also existed, however, with respect to new credit card accounts.<sup>23</sup> Both of these outcomes are logical, given that consumers generally are not liable for unauthorized uses of their credit card.<sup>24</sup>

A very different story is reported in the media and even by state regulators. For example, a California regulator describes the same 2003 FTC Report this way: “The costs of the crime are alarming. Recent studies estimate the

average victim’s out-of-pocket expenses at \$500 to \$740, and the time spent clearing up the situation at from 30 to several hundred hours”.<sup>25</sup> While that is true, it is out of context and quite misleading. As noted, the FTC report says that for 63 percent of victims, that is, a sizable majority, there was no loss of money at all, and that is shown on the following copy of the report’s graphic. In the graphic, the first group of vertical bars is where the 63 percent average comes from, that is, a majority of victims suffered no loss. Thus, the median of all victims have zero loss; the mean would be higher. The California regulator obtained its \$500 number by focusing solely on the third group of vertical bars in the chart, but did not put that group into context.



In any event, statistics are just that and no one would want to fall within them even if they are not as alarming as portrayed by regulators with an agenda. Also, the fact that the “victim” suffered little or no financial loss does not mean that a loss did not occur for someone. Retailers, card companies and others may have suffered some loss even though the “victim” that is the focus of these statistics did not.

The problem caused by exaggeration, however, is the response it creates – that is, overreactive legislation that is passed in haste or based on false assumptions. This is particularly troublesome with identity theft because there are two victims, not just one. The victim treated by most legislation is the one whose identity is stolen; but the second victim is the business victim who is duped: each deserves consideration and exaggeration tends to preclude that.

While reasonable minds may differ regarding the actual facts about identity theft. Laws are increasing at a rapid rate. In the United States, a massive new law has been adopted, the Fair and Accurate Credit Transactions Act of 2003<sup>26</sup> (“FACT”). It focuses on consumer reporting agencies (aka credit reporting agencies) and use of credit reports and credit scores. However, it also contemplates a much broader application that will affect essentially every entity engaging in U.S. commerce for consideration – each such business must establish procedures to respond to consumer claims of identity theft. It also affects other issues such as the ability to sell or transfer debt involving identity theft; what may be printed on a receipt for a credit or debit card; how change-of-address requests for credit or debit cards may be processed; sharing of consumer information among affiliates; and limitations on the use of medical information and so on.<sup>27</sup> FACT imposes or increases procedural and substantive requirements on disclosure and use of credit reports and credit scores and on businesses that deal with identity thieves. In addition to being a complex statute in itself, FACT contemplates the issuance of extensive regulations by the FTC or other regulators supporting its provisions.

## What Other U.S. Laws Address Identity Theft?

In addition to FACT, a wide range of federal and state laws relate to identity theft. Some specifically address identity theft as a crime and some can be used to charge identity thieves with other related crimes. There are also “privacy or data collection” laws that can help prevent identity theft by regulating how personal information can be collected and when it can be disclosed, or help identity theft victims restore their credit ratings and limit their liability for unauthorised debts. Identity theft is also one of the suspected criminal violations that require a U.S. financial institution to file a “suspicious activity report”.

### Policy Issues

Two general points should be made laws before turning to laws specifically related to identity theft. First, at times the risk of identity theft will have to give way to other public policies. Second, laws regarding privacy and identity theft are pushing in opposite directions and will, inevitably, clash. This may be true in other countries as well, but it particularly true in the United States because of the heavy policy emphasis, both constitutionally and by culture, on the free flow of information.

## Identity Theft vis a vis Other Public Policies

*In re Crawford*<sup>28</sup> is illustrative of the point that the risk of identity theft may have to give way to other U.S. public policies. In this Ninth Circuit case, the court examined the disclosure, as opposed to the collection, of social security numbers. It started with the premise that a constitutional “zone of privacy” has been firmly established by the U.S. Supreme Court although the boundaries of that zone are not clear:

We have observed that the relevant Supreme Court precedents delineate at least two distinct kinds of constitutionally-protected privacy interests: “One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions”.<sup>29</sup>

The court noted that not all circuits agree and that some have “disavowed the notion of *informational*<sup>30</sup> privacy as a constitutionally protected interest.” The court characterised that as the minority view and inconsistent with the law of the Ninth Circuit.<sup>31</sup> It then turned to the question at hand, which was whether a federal bankruptcy statute was unconstitutional because it required non-attorney preparers of bankruptcy petitions to list their social security number. A preparer alleged that this was unconstitutional because the petition became a public record, and such a forced disclosure of his SSN exposed him to crimes such as identity theft. The court agreed that the “indiscriminate public disclosure of SSNs, especially when accompanied by names and addresses, may implicate the constitutional right to informational privacy”.<sup>32</sup> However, that right must be weighed against the governmental interests underlying the statute, and the court concluded that those outweighed the preparer’s interests.<sup>33</sup> The “speculative possibility of identity theft is not enough to trump the importance of the governmental interests behind” the federal statute and the court could not say that Congress transgressed the bounds of the Constitution in enacting the statute.<sup>34</sup>

Public policies come in various shapes and sizes. An obvious one is the policy of preventing identity theft itself or other crimes or terrorism. As laws are enacted to address one aspect of a particular policy, that very law may exacerbate problems under other aspects of the same or a different policy. For example, the federal Fair and Accurate Credit Transactions Act of 2003 (FACT), in an effort to assist victims of identity theft, imposes significant obligations to adopt procedures to avoid errors and resolve disputes on various persons, including those furnishing information to a consumer reporting agency and persons using consumer reports from those agencies. A logical response for a business subject to those obligations and regulations would be to cease using or providing shared information. But the effect of that will, in fact, clash with the public policy of preventing identity theft and other crimes.

To illustrate, assume an identity thief opens five new accounts in a single week, having stolen the identity of John Doe. Three of the accounts are opened at a telephone company, a department store, and a car rental agency, each of which has determined not to obtain credit reports from consumer reporting agencies and not to provide information to them, all in order to avoid the procedural and other obligations imposed by, and legal compliance costs of, FACT. Each has weighed the costs of compliance against the likelihood of dealing with an imposter and has determined simply to avoid sharing information. Thus, the

information about John Doe from those three companies will not enter the reporting system and will not be available to be noticed by either of the other two businesses that are obtaining consumer reports or reporting information and checking for indications of fraud (such as any unusual frequency of account openings or activity by John Doe). Information about John Doe will simply drop out of the reporting system and soon the thief will have an open field to commit even more identity thefts. Competing policies are at work and dealing with one may adversely impact the other.

## Collision of Identity Theft and Privacy

Laws regarding privacy and identity theft are pushing in opposite directions and will, inevitably, clash. We discuss below a California statute<sup>35</sup> allowing the imposition of a \$30,000 penalty on a vendor who, as a victim itself of identity theft, continues to pursue its claim against the other victim (the person whose identity has been stolen) after the vendor has been presented with facts that later entitle the other victim to obtain a judgment eliminating the purported obligation. Similarly, FACT requires various levels of proof of identity in order to complete a transaction or provide certain information, including a “high degree of confidence” that one is dealing with the correct person.

These kinds of statutes send this message to vendors and service providers: “unless you find ways actually to prove with whom you are dealing, you will suffer not only the loss of an unauthorized transaction, but will also be heavily penalized.” The obvious and legitimate response by vendors and service providers is to require significantly more identification before entering a transaction or a relationship. But when the vendor collects that additional information, it will run into claims that the collection violates the customer’s privacy. This places the vendor in the classic position - living between a rock and a hard place.

How this will play out in the courts is not yet known. Two cases are illustrative. In *Messing v. Bank of America*,<sup>36</sup> a bank was sued by a payee of a check. The payee went to the drawee bank and sought its acceptance of the check and payment. That bank was part of a program intended to reduce check fraud and had a stated policy of requiring non-customers to provide a thumbprint on a device leaving no ink stains. The payee refused to provide the print, claiming that this would violate his right to privacy and that it was not the kind of identification contemplated by Uniform Commercial Code (UCC) Article 3, the law in each U.S. state regarding payments by check. The court had to decide whether the bank could be viewed as having “dishonored” the check by requiring the thumbprint: UCC Article 3-501(b)(2)(ii) allows a bank to request “reasonable identification” and if the request is reasonable, then there is no dishonour under UCC Article 3-501(b)(3)(ii). The payee argued it was not reasonable: He had already presented a credit card and driver’s license which the bank had entered on the back of the check; also, even if he supplied a thumbprint, that would not tell the bank who he was at the time of payment – it would only be useful later. The court disagreed, noting that other courts had determined that requiring a thumbprint was not an invasion of privacy in non-criminal contexts, and concluding that even if a thumbprint does not provide immediate identification, it

does provide a powerful deterrent to those who might attempt to pass bad checks. It held that this reduction of risk promotes the expansion of commercial practices contemplated by the UCC and that the bank’s requirement of a thumbprint by non-customers was reasonable.<sup>37</sup>

*Messing* illustrates that as adverse consequences are allocated to service providers, they will respond by requiring more identification and that at some point, customers will claim that the new requirements invade their privacy.

Ironically, that debate will be complicated by the fact that consumers will also claim that the service provider should have requested *more* information and is liable for not doing so. *Andrews v. TRW, Inc.*<sup>38</sup> is illustrative of consumer claims even though it was ultimately reversed. There, the victim of identity theft sued TRW, a credit reporting agency, for supplying credit reports to vendors who believed they were dealing with the victim but were actually dealing with the thief. Under the Fair Credit Reporting Act (FCRA), TRW could only furnish a credit report when it had “reason to believe” the report would be used in connection with a credit transaction involving the subject of the report. It argued it had fulfilled this obligation by supplying the report after receiving the name and social security number of the supposed customer. The lower court granted summary judgment, reasoning that the random chance of those two data elements matching, given the universe of names and numbers, was very small.<sup>39</sup> The Ninth Circuit reversed and remanded, concluding that the issue was a question of fact and that a jury should decide “whether identity theft has been common enough for it to be reasonable for a credit reporting agency to disclose credit information merely because a last name matches a social security number on file.”<sup>40</sup> The standards set in FCRA are statutory and higher than those that tend otherwise to be set in ordinary commerce, and the amendment of FCRA by FACT directly or indirectly mandates the collection by businesses of ever more identifying information. Thus, the dilemma remains: Customers will argue both for and against more privacy and this will create tension under identity theft statutes and procedures necessary to attribute acts to particular persons. Confusion is certain; answers are not.

## U.S. Federal Criminal Statutes

### *The Identity Theft and Assumption Deterrence Act of 1998*

The federal Identity Theft and Assumption Deterrence Act of 1998<sup>41</sup> specifically labels identity theft as a crime. Prior to the act’s passage, 18 USC 1028(a) criminalised the unauthorised use or transfer of identity documents such as a social security card, and 18 USC 1029 made illegal the unauthorised use of credit cards, ATM (automated teller machine) codes, and the like.<sup>42</sup> While those sections continue in force, the act added a new subsection, 18 USC 1028(a) (7), which applies when a person “knowingly transfers or uses, without lawful authority, a *means of identification* of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. . . .” The act defines “means of identification” as:

...any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any –

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device (as defined in section 1029(e)).<sup>43</sup>

This broadened the scope of 18 USC 1028(a) to include the misuse of information while retaining use or transfer of documents such as a social security card. Thus, the statute has recognised since 1998 that criminals do not need documents to assume an identity – “often they just need the information itself to facilitate these types of crimes.”<sup>44</sup> The fact that this expansion was necessary is not surprising and, in fact, is symptomatic of the information age: Most U.S. laws, including commercial laws such as UCC 2 (sales of goods), were written with tangible objects in mind such as the social security card, as opposed to the information, and cannot be or should not be applied to information.<sup>45</sup>

### Other Laws

The Identity Theft and Assumption Deterrence Act of 1998<sup>46</sup> can be applied to a wide range of offences that can be independently prosecuted under the act or other numerous statutes. For example, the unauthorised use of credit cards was already illegal under 18 USC 1029, but after 1998, it can be prosecuted under that section or under the act. “In total . . . the violation of some 180 federal criminal statutes can potentially fall within the ambit of 18 USC 1028(a)(7).”<sup>47</sup>

Most states have also enacted laws criminalising identity theft: about forty-four states have specific laws, and five others have laws covering activities “included within the definition of identity theft”.<sup>48</sup> According to the FTC, identity theft crimes can be considered felony offences in forty-five of the forty-nine states that have relevant laws.<sup>49</sup> The previously noted federal Fair and Accurate Credit Transactions Act<sup>50</sup> will preempt some of the state laws in varying degrees. But FACT itself if a comprehensive new law regarding identity theft.

## How Can Potential Victims Decrease the Risk of Identity Theft?

The FTC 2003 Report indicates several things that potential victims of identity theft can do to forestall it. All harmful repercussions seem to be reduced by prompt discovery of misuse, such as examining monthly statements of accounts: 52 percent of all victims cited this as the way that they discovered they were victims of identity theft.<sup>51</sup> Other suggestions made by those surveyed for the report included:

Many victims thought better awareness on their own part of how to prevent and respond to identity theft would have been most helpful. Specific areas where greater awareness was cited included taking greater security precautions in handling their personal information, such as destroying materials that contain personal information instead of simply

putting them in the trash, not placing personal information on the Internet, and securing their personal information in their homes and at work. Maintaining greater vigilance, such as monitoring their mail, billing cycles, and credit reports more carefully was also cited. Lastly, knowing who to contact, and notifying the affected companies and credit reporting agencies more quickly when they detected something wrong, was identified as an important factor in recovering from identity theft.<sup>52</sup>

- 1 For a discussion of the various methods established by U.S. law to “attribute” acts to a particular person, see Chapter 6 of Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003).
- 2 FTC Identity Theft Survey Report at 9 and 30, prepared by Synovate (September, 2003) (copy available at [www.ftc.gov/os/2003/09/synovate-report.pdf](http://www.ftc.gov/os/2003/09/synovate-report.pdf), visited 19/08/04) (hereafter, “FTC 2003 Report”). This was 25 percent of those who actually knew how their information was obtained. This group accounts for 51 percent of all victims (leaving almost half of victims not knowing how their information was obtained). Id. at 9 and 30.
- 3 See “Big Trust in Database Leads to Big ID Thefts,” Mark Jewell, *The Seattle Times* at D2 (8/10/04).
- 4 Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc., *Identity Fraud: A Critical National and Global Threat* at 4 (October 28, 2003) (copy available at [www.ecii.edu/identity\\_fraud.pdf](http://www.ecii.edu/identity_fraud.pdf)).
- 5 S.B. Hoar, “Identity Theft: The Crime of the New Millennium”, 80 Or. L. Rev. 1423, 1423 (2001).
- 6 FTC 2003 Report at 7. The 4.6 percentage figure converts to 9.91 million people. California regulators view this number with much more alarm, using it as a basis for guidance issued in connection with a California statute requiring notice when there is a breach of security of certain computerised systems. “A national survey conducted by the Federal Trade Commission found that the number of victims in 2002 approached 10 million, and two other recent surveys estimated the number at seven million. That’s nearly 10 times greater than the previously quoted estimate of less than a million a year. If the same rate is applied to California, then over a million Californians became victims of identity theft in the past year.” See CA Office of Privacy Protection, Recommended Practices on Notification of Security Breach Involving Personal Information at 5, regarding CA Civil Code 1798.82. On the other hand, identity theft is the most complained about crime based on reports made to the FTC. See FTC National and State Trends in Fraud and Identity Theft (1/2004), copy available at [www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf](http://www.consumer.gov/sentinel/pubs/Top10Fraud2003.pdf).
- 7 S. Rep. No. 05-274, at 7 (1998).
- 8 See settlement order in *FTC v. James D. Thompson and Susan B. Germek* (ND of Illinois, Eastern Division), Case No. 0C3 2541; FTC File No. 032 3096.
- 9 NACHA Internet Council, *Internet Payments Fraud: A Primer for Merchants and Financial Institutions* (Feb. 3, 2003) (copy available at <http://internetcouncil.nacha.org/docs/Fraud%20Paper%20Final%20%20Jan%20%2703.pdf>, visited 19/08/04).
- 10 *FTC v. James D. Thompson and Susan B. Germek* (ND of Illinois, Eastern Division), Case No. 0C3 2541; FTC File No. 032 3096 at 9.
- 11 See Joint Project of the Economic Crime Institute of Utica College and LexisNexis, a Division of Reed Elsevier Inc., *Identity Fraud: A Critical National and Global Threat*, (October 28, 2003). Copy available at [www.ecii.edu/identity\\_fraud.pdf](http://www.ecii.edu/identity_fraud.pdf). This white paper defines identity fraud as follows:
 

“Identity fraud, which encompasses identity theft, is the use of false identifiers, false or fraudulent documents, or a stolen identity in the commission of a crime. It often emanates from a breeder document created from fictitious or stolen identifiers. The breeder document, such as a driver’s license or birth certificate, is used to spawn other documents, resulting in the creation of a credible identity which allows a criminal or terrorist access to credit cards, employment, bank accounts, secure facilities, computer systems, and the like.”
- 12 Id. at 13.

- 13 See [www.idtheftcenter.org/alerts.shtml](http://www.idtheftcenter.org/alerts.shtml).
- 14 NACHA Internet Council, Internet Payments Fraud: A Primer for Merchants and Financial Institutions (Feb. 3, 2003) (copy available at <http://internetcouncil.nacha.org/docs/Fraud%20Paper%20Final%20%20Jan%20%2703.pdf>, visited 19/08/04).
- 15 See CDT January, 2004 letter regarding: *2003 Reports of Internal Fraud and Physical Security Problems at State Motor Vehicle Offices* (organised by state), copy available at [www.cdt.org/privacy/20040200dmv.pdf](http://www.cdt.org/privacy/20040200dmv.pdf) (as of 1/04), at 28.
- 16 *Id.*
- 17 *Id.* See, e.g., *Andrews v. TRW Inc.*, 225 F3d 1063 (9th Cir. 2000), rev'd, 534 U.S. 19 (2001) (involving identity theft by receptionist in doctor's office of information supplied by the patient to the doctor; reversed as barred by statute of limitations).
- 18 *Id.*
- 19 FTC 2003 Report at 43.
- 20 *Id.* at 45. Some 29 percent required two to nine hours; 30 percent required more than ten hours; and six percent spent over 240 hours. *Id.*
- 21 *Id.* at 15. Slightly less than half (44 percent) said they were "very" or "somewhat" concerned that they will be victimised.
- 22 *Id.* at 52. Misuse of existing credit cards accounted for 56 percent of all identity theft victims; of those, 73 percent were "very satisfied" with how the credit card company responded to the report of misuse. *Id.* Where more than one existing credit card was misused, or a new credit card was misused, satisfaction levels dropped to 53 percent. *Id.*
- 23 *Id.* at 52–53. Victims of new account experienced slightly lower levels of satisfaction but still, 78 percent were satisfied.
- 24 See Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003) at ¶ 6.06.
- 25 See CA Office of Privacy Protection, Recommended Practices on Notification of Security Breach Involving Personal Information at 5, regarding CA Civil Code 1798.82.
- 26 Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (December 4, 2003), hereafter "FACT".
- 27 For a full discussion of FACT and these topics, see Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003) at Chapter 15.06[3] and chapters cited therein.
- 28 In re Crawford, 194 F3d 954 (9th Cir. 1999), cert. denied sub nom *Ferm v. U.S. Trustee*, 528 US 1189 (2000).
- 29 *Id.* at 959.
- 30 The discussion here focuses only on "informational" privacy as opposed to more traditional forms of privacy. There is myriad U.S. law, federal and state, on traditional notions of privacy. See discussion in Chapter 6 of Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003), Chapter 12.
- 31 194 F3d 954 at n. 4.
- 32 *Id.* at 959. The court discussed the harm that can flow from misuse of social security numbers and distinguished them from names and telephone numbers because the SSN serves as a unique identifier that cannot be changed and is not generally disclosed by individuals to the public. *Id.*
- 33 *Id.* at 961 (legislative purpose of protecting persons filing bankruptcy from unlicensed preparers and benefits of public access to bankruptcy records).
- 34 *Id.* at 961. The court did note in footnote 9 that the preparer had raised valid privacy concerns and encouraged Congress to consider enacting rules to limit the disclosure of preparer SSNs.
- 35 California Civil Code 1798.92 through 1798.97.
- 36 *Messing v. Bank of America, NA.*, 373 Md. 672, 821 A2d 22 (2003).
- 37 *Id.* at 40.
- 38 *Andrews v. TRW, Inc.* 225 F3d 1063 (9th Cir. 2000), rev'd, 534 U.S. 19 (2001).
- 39 *Id.* at 1067.
- 40 *Id.* at 1067. The court also said the jury should assess whether the question of reasonableness was affected by information possessed by TRW such as the misspelling of the supposed customer's first name and a mistake in the birth date. "A jury will have to say how reasonable a belief is that let a social security number rump all evidence of dissimilarity between the Plaintiff and the Imposter." *Id.*
- 41 18 USC 1028 (2003).
- 42 GAO, Identity Theft: Greater Awareness and Use of Existing Data Are Needed at 5 (June 2002).
- 43 *Id.*
- 44 S. Rep. No. 105-274, at 6 (1998).
- 45 This topic is the subject of debate in the U.S. as courts and legislatures struggle to draw appropriate dividing lines and free themselves of thinking that works for "goods" but not for "information." See, e.g., *U.S. v. Stafford*, 136 F3d 1109, 1115-1116 (7th Cir. 1998), modified, 136 F3d 1115 (7th Cir. 1998) and cert. denied, 525 U.S. 849 (1998), in which the court said:  
The government concedes that the codes are not securities or money, but it says that they are goods, wares, or merchandise. They're not; they're information. No doubt Allison wrote them down rather than committing them to memory, but he was not charged with having transported pieces of paper containing codes across state lines and we need not decide whether such transportation would violate the statute. He was charged with transferring the codes themselves, which are simply sequences of digits. The sequences have no value in themselves; they are information the possession of which enables a person to cash a check.  
See also *Specht v. Netscape Communications Corp.*, 306 F3d 17, note 13 (2d Cir. 2002), stating, "Recognizing that 'a body of law based on images of the sale of manufactured goods ill fits licenses and other transactions in computer information', the National Conference of Commissioners on Uniform State Laws has promulgated the Uniform Computer Information Transactions Act (UCITA), a code resembling UCC Article 2 in many respects but drafted to reflect emergent practices in the sale and licensing of computer information".
- 46 18 USC 1028 (2003).
- 47 18 USC 1028 (2003).
- 48 GAO, *Identity Theft: Greater Awareness and Use of Existing Data Are Needed*, at 1, 6. Vermont was the only state that does not have a law that either specifically addresses identity theft or covers activities included within the definition of identity theft. See Chapter 15 of Holly K. Towle and Raymond T. Nimmer, *The Law of Electronic Commercial Transaction* (A.S. Pratt & Sons, 2003) (listing the states and the relevant state laws, as well as more federal statutes).
- 49 *Id.* at 6. Of those states that have not passed identity theft legislation, many are considering doing so. FTC, *ID Theft: When Bad Things Happen to Your Good Name 1* (Sept. 2002), available at [www.ftc.gov/bcp/online/pubs/credit/idtheft.pdf](http://www.ftc.gov/bcp/online/pubs/credit/idtheft.pdf) at 25.
- 50 Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 (December 4, 2003).
- 51 FTC 2003 Report at 39. Some 25 percent were notified by their account institution or other vendors who noticed suspicious account activity; eight percent discovered they were victims when they were turned down while attempting to obtain credit; and nine percent knew they had lost their information because they had lost a wallet or purse. *Id.* at 39 and 40.
- 52 FTC 2003 Report at 62. For a list of recommendations regarding avoidance of identity theft, see Holly K. Towle and Raymond T. Nimmer, *Law of Electronic Commercial Transactions*, Chapter 15.07 (A.S. Pratt & Sons 2003).

*Holly is the co-author of Holly K. Towle and Raymond T. Nimmer, The Law of Electronic Commercial Transaction (A.S. Pratt & Sons, 2003) an information rich treatise explaining the legal landscape of electronic commercial law (www.sheshunoff.com/store/F53.html). For a more complete treatment, please see that publication or see Towle, Holly, "Identity Theft: myths, methods and new laws"; The Rutgers Computer and Technology Law Journal, 30 RUTGERS COMPUTER & TECH. L.J. 237 (2004).*