Identity Theft: Developments in Third Party Liability

By: Stephen L. Wood and Bradley I. Schecter

An estimated 700,000 people were victimized by identity theft in the year 2000, making it one of the most common, and costly, crimes today. While identity theft is hardly new, law enforcement officials and consumer advocates say the Internet is making identity theft one of the signature crimes of the digital era. Anyone with access to the Internet can find websites selling all sorts of personal information and, with that information in hand, thieves can acquire credit and make purchases using someone else's identity and credit.

The costs can be significant and long lasting for individuals who are victims of identity theft. Identity thieves can run up debts in the tens of thousands of dollars under their victim's name and credit, and, even though the victim may not legally be responsible for those debts, the consequences of the thief's actions are often considerable. A person's credit history can be virtually destroyed, significantly impairing the individual's ability to obtain credit loans, mortgages, and employment. A bad credit report may even prevent someone from obtaining something as simple as a checking account. In addition, it may take a victimized consumer numerous months and significant personal expenses to contest all of the fraudulently obtained charges and to correct the credit reporting errors.

Despite all of this hardship, however, in a typical identity theft case, law enforcement officials do not consider someone whose identity was stolen to be the "victim." The logic is this: if the consumer is not legally obligated to pay any of the bills the imposter incurred, the consumer has not lost any money. That rationale, however, fails to provide recourse to those individuals who have had their identity stolen and have endured the time consuming and expensive task of restoring their good name and credit.

This article looks at the causes of identity theft and explores the cases that have imposed third party tort liability on banks and financial institutions who arguably facilitated or enabled the fraud to occur. The emerging trends suggest that if banks and financial companies want to insulate themselves from such claims, they may need to take additional steps to prevent identity theft.

- How Identity Theft Happens

Identity theft occurs when someone uses the identifying information of another person — name, social security number, mother's maiden name, or other personal information — to commit fraud or engage in other unlawful activities. For example, an identity thief may open a new credit card account under someone else's name. When the identity thief fails to pay the bills, the bad debt is recorded on the other individual's credit report. Some common methods and means of economic identity theft are identified below.

- Account Takeover Fraud

Account takeover fraud occurs when the identity thief fraudulently uses an existing deposit or credit account of a consumer without the consumer's consent or, often, without his or her knowledge. The thief might steal a consumer's bill or account statement and then contact the financial institution to provide a "new" address for the account. The consumer is unlikely to know of the change until the next statement date or when the account becomes past due or overdrawn. That delay gives the thief time to use the account without the account being flagged or the fraud detected. In addition, the identity thief can steal funds directly from an individual's account by impersonating the individual and effecting a wire transfer or by making credit card purchases or cash advances over the Internet or telephone. The theft can even occur by cashing in an investment holding or insurance policy.

- Fraudulently Opening New Accounts

Another common method of identity theft occurs when a perpetrator steals an application for a credit card or account and opens an entirely new account in another's name. This theft can easily occur when an identity thief steals a credit
card application from a consumer's mailbox. Given the large number of unsolicited "pre-approved" credit card applications that arrive almost daily in some consumer's mailboxes, there are ample opportunities to obtain such applications, and consumers are unlikely to notice that an unsolicited credit offer was missing from the mailbox. Once the thief has the application, he or she fills it out in the consumer's name, but uses a different address. This fraud allows the perpetrator to use the credit card without being detected for quite some time; the consumer does not know that the new credit card was issued until he or she is notified by a credit agency or is tracked down by a bill collector.

- **Pretext Calling and Other Methods For Gaining Necessary Personal Information**

Each of the above mentioned schemes is easier to effectuate if the thief also is able to gain important, confidential information about the "victims." This information includes data that banks and other financial institutions have access to and utilize in the course of their business and is also the data needed to change information on accounts (such as billing addresses). Crucial information for an identity thief includes social security numbers, maiden names, dates of birth, and driver's license information. One way thieves get this information is through pretext calling.

Pretext calling involves obtaining confidential consumer information under false pretenses, e.g., by lying and pretending to be the consumer. Pretext calling occurs when the caller identifies himself as the consumer to the bank or other financial about "his own" account. Using some basic information about the consumer (such as current address, date of birth, and/or social security numbers), a thief can get a bank to divulge additional data such as the consumer's account number, account balance, payment history, and the dates and amounts of recent transactions. That information, in turn, can enable the thief to take over accounts or open new accounts at a later time. Another type of pretext calling involves the thief pretending to be an officer of a financial company, and calling the consumer to elicit personal or confidential information, such as passwords and account numbers. Unless the financial company already has established with the consumer a protocol for such interactions, the consumer might not be aware that he or she is dealing with a thief instead of the company.

Pretexting is not the only means by which identity thieves can obtain confidential and personal information about their prospective "victims." Other methods include retrieving statements and receipts from a consumer's trash, or even looking through a co-worker's desk drawer. In addition, the Internet has become a source where thieves, for the right price, can obtain social security numbers and other identifying data from unscrupulous "personal data" merchants.

- **Financial Institutions and Third Party Liability for Identity Theft**

Although law enforcement consider banks and financial institutions to be the "victims" in identity theft cases (unless insured, they frequently are forced to absorb the costs of the thefts), a few recent cases have suggested that current business and marketing practices of companies may negligently lead to identity theft. As a result, financial institutions now face potential third party tort liability in identity theft cases.

The business practices in question grow out of the highly competitive nature of the credit card industry. Companies fighting for new customers and greater market share routinely offer "instant" credit, in addition to unsolicited and pre-approved credit cards. As these practices continue, consumers are beginning to turn to financial companies to recover their losses from identity theft, arguing that the companies' weak standards and overly aggressive marketing practice enabled the theft to occur.

Like most negligence claims, to hold a bank or financial institution liable, a consumer must prove: (1) the bank or credit agency committed some act that enabled or helped the identity theft to occur; (2) that the bank or credit agency owed a duty to the consumer whose identity was stolen; (3) that the bank or credit agency breached that duty; and (4) that the breach was
the actual and proximate cause of the consumer's injury. Each element is addressed below.

- **Enabling the Theft**
  A financial institution can subject itself to potential liability for identity theft by negligently making the offer of credit or negligently granting credit to an identity thief. In addition, a bank or credit agency may be subjected to pretext calling — negligently releasing personal, confidential information that helps to enable the identity theft to occur.

- **The Duty of the Financial Institution to the Customer**
  Courts have struggled to advance a consistent theory for imposing duties on financial institutions with respect to the disclosure of consumer information. Some courts have imposed a common law duty on financial institutions to preserve the confidentiality of customer financial records based on an implied contract of financial privacy between a financial institution and its customers. An early case, *Peterson v. Idaho First National Bank*, illustrates such an implied contract. In *Peterson*, the consumer sought recovery for "invasion of privacy" when the manager of the bank where the consumer had a checking account disclosed to the consumer's employer that the consumer had bounced checks on the account. The Idaho Supreme Court affirmed the dismissal of plaintiff's invasion of privacy claims, but held that the facts supported a claim for breach of an "implied contract" between the consumer and the bank. Finding it "inconceivable that a bank would at any time consider itself at liberty to disclose the intimate details of its depositors' accounts," the court concluded that no financial information may be disclosed to third parties unless authorized by law or by the customer. *Peterson* was thereafter cited for the proposition that there was a common law "contract" duty on banks and financial institutions not to disclose confidential information about a consumer's accounts and that unauthorized disclosures could lead to liability for breach of the implied contract.

  Other courts have moved beyond the implied contract theory and have held that violations of the bank's duty of confidentiality could lead to tort liability, and even punitive damages. In *Djowharzadeh v. City National Bank & Trust Co.*, a bank employee divulged a customer's confidential, financial investment information to the bank president's wife, who used the information to secure an investment opportunity at the consumer's expense. The court reasoned, "[t]his intimate, private information is not furnished to any bank official lightly, nor strictly speaking, voluntarily. Rather, the borrower is compelled to disclose the information." In ruling that a duty of confidentiality exists between the two, the court relied heavily on the public policy needs of assuring that banks and financial institutions will keep highly sensitive customer information confidential. The court concluded that the facts alleged by the consumer could support actions under tort or contract theories.

  Although the foregoing cases do not specifically involve third party liability for identity theft, these cases provided the foundation on which the later identity theft cases were built. Once courts had recognized that certain non explicit duties might exist (in both tort and contract) between financial institutions and their customers, the next step to third party liability was incremental rather than monumental.

  The Alabama Supreme Court recently addressed head-on the existence of third party liability for identity theft. In *Patrick v. Union State Bank*, the plaintiff sued her bank, alleging that it negligently allowed an imposter to open a checking account in her name and write numerous bad checks on the account. Plaintiff established that the bank allowed the imposter to open the account using only one form of identification — the plaintiff's stolen, photo-less temporary driver's license. Not only did the bank employee ask for only one form of identification, she did nothing when the thief gave no permanent address, did not act when she noticed that the signatures on the application and the driver's license did not match, did not ask the imposter to verify the Social Security number by presenting a Social Security card, and did not attempt to verify any of the telephone numbers given.

  In finding that the bank owed a duty to the plaintiff in *Patrick*, the court stated that duty in
an identity theft context should be analyzed according to traditional principles. 19 Quoting earlier authority, the court held that a duty did exist because "[b]lanks stand in the intimate relation of a fiduciary to those who are their customers, depositors, stockholders, and associate banks, as well as the public generally, whose members are affected by their operation." 20

The Patrick court cautioned that, read literally, the foregoing language arguably established a rule that banks owed fiduciary duties to the public at large. The Patrick court did not go that far, but ruled that "the nature of the activity of a bank...is such that duty to the public in the exercise of the bank's business maybe justifiably imposed." 21 Further, the court stated that the "imposition of tort liability is appropriate" because "the fraudulent scheme effectuated here, as well as the injury and harm it caused Patrick, was foreseeable to the extent that a duty may be imposed." 22 The court concluded: "It is foreseeable to banks that failing to follow identification procedure will greatly increase the risk of fraud." 23 Patrick clearly illustrates that courts are willing to look beyond traditional notions of thief and "victim," and to impose third party liability on a bank or financial institution whose business practices facilitated the consumer victim's injuries.

- The Breach Leading to the Identity Theft

Finding that a duty exists between the financial institution and the consumer victim is only part of the battle — for third party liability to exist, it also must be found that the bank, for example, breached that duty by negligently enabling the identity theft to occur. A plaintiff must prove that the actions undertaken by the bank to release financial information, provide financial information to vendors for marketing purposes, or extend credit, were unreasonable.

Few reported cases define what is considered "unreasonable." In the Patrick case, the court suggests that it was commercially unreasonable for the bank to ignore established identification policies and to fail to verify the authenticity of signatures. 24 It is not known, however, how lax a bank's security procedures in issuing credit or in divulging consumer information must be before a court will hold it liable for any resulting identity theft. Nor does the Patrick case shed light on what "established identification policies" provide. Plaintiff's security expert had testified that photographic identification and a comparison of signatures was standard. 25 But beyond those fairly prosaic rules, little additional guidance can be gleaned from the decision. Until more cases are decided, or legislatures enter the fray, this issue remains a somewhat open question. What seems clear now, however, is that banks and financial institutions operate at their peril when they disregard established security measures designed to limit the disclosure of confidential consumer information or extend credit without sufficient verification. 26 Of course, as technology evolves and new methods of identity theft are devised, financial institutions will need to keep abreast of developments and adjust their security measures to prevent improper access.

- The Financial Institution Causes the Plaintiff's Injury

In addition to duty and breach, a plaintiff also has to prove that the institution's negligence proximately and actually caused damage. That task is more difficult than expected for one whose identity has been stolen, because, as noted above, law enforcement officials still view the banks and credit companies as the true victims of the theft. Patrick, however, does provide some hope for plaintiffs. The court there denied summary judgment for the bank on the issue of causation, stating that the bank should have realized the likelihood that its opening of a checking account based solely on the presentation of a photo-less temporary driver's license as identification, without verifying any of the information given, would lead to an opportunity for an imposter to write worthless checks and thereby damage the consumer. 27 The consumer's damages arising from the breach, which in Patrick were valued inter alia as the consumer's repeated arrests for bouncing checks which she did not write, were held to be compensable. Patrick opens the door for future tort actions in which more typical damages (time, money, energy expended in restoring good credit, for example) will be held compensable.
• Current Federal Statutes and How They Interact With Identity Theft

Although in recent years some federal statutes have been enacted concerning the maintenance and protection of consumer information, none of them is particularly useful regarding the issue of third party tort liability in identity theft cases. That is, none of them defines the specific obligations a financial institution must undertake to protect consumers from potential identity theft, and none of them establishes a cause of action for consumers to seek damages from such institutions for enabling or facilitating such crimes.

• The Gramm-Leach-Bliley Act

As part of larger legislation revision federal financial services law, Title V of the Gramm-Leach-Bliley Act imposes on financial institutions an affirmative and continuing obligation to protect consumer privacy and limits the ability of these institutions to share nonpublic information. The Act recites general standards that must be met, such as insuring the security and confidentiality of customer records and information, protecting against anticipated threats or hazards to the security of the records, and protecting against unauthorized access to or use of records which could result in substantial harm or inconvenience to any customer. Several federal banking regulators issued guidelines to implement the security provisions; other independent agencies such as the SEC and FTC have issued regulations.

The Act's privacy provisions do not, however, limit the sharing of consumer information among "affiliated" institutions, and require the consumer to affirmatively "opt out" of the disclosure provisions if the consumer wishes to prohibit transmission of his or her personal information to a "nonaffiliated" third party. If a consumer does not "opt out" of allowing the sharing of his or her personal information, and is later victimized by it, and if the disclosure could be traced back to a specific financial institution (which would be difficult, if not impossible), will the consumer's failure affect his or her negligence action against the financial company? Again, until the courts start ruling on cases involving the Gramm-Leach-Bliley Act, these answers remain elusive.

• The Fair Credit Reporting Act

The Fair Credit Reporting Act (the "FCRA") is the most heavily cited statute in identity theft cases. The FCRA establishes standards for the collection, maintenance, and disclosure of consumer credit information by consumer credit reporting agencies, and it allows for a civil action against an institution that violates the statute. However, the FCRA fails to define the "reasonable procedures" that a credit agency must follow to protect a consumer's information.

One example of how the FCRA has been used to attack allegedly lax procedures of financial institutions is Andrews v. TRW. In Andrews, the plaintiff sued TRW, the consumer credit reporting agency, after an imposter used her social security number to obtain credit cards issued in the imposter's name. TRW approved the extension of credit even though the thief used her own personal information, except for plaintiff's social security number and in one application used a misspelling of plaintiff's first name. The plaintiff sued under the FCRA, claiming that TRW improperly had furnished credit reports without "reasonable grounds for believing" that she was the consumer whom the credit applications involved. The court allowed the suit to continue, holding that it was for the "jury to 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." The court noted that "the jury would be helped by expert opinion on the prevalence of identity theft" in making its determination.

Before the case went to trial on Andrews' claim that TRW lacked reasonable grounds for believing that she was the consumer whom the credit applications involved, the Supreme Court granted certiorari on a statute of limitations issue. The Supreme Court reversed the Ninth Circuit's holding that the two year statute of limitations did not begin to run until Andrews knew or should have known she was injured. This ruling limited Andrews' claims, but the Supreme Court did not disturb the court of
appeals' holding on the need for a trial on Andrews' remaining claims. Thus, the court's analysis in Andrews suggests that financial institutions need to reevaluate their current practices for extending credit to ensure that such practices are sufficient, in light of the availability of social security numbers, to prevent common forms of identity theft.

- The Identity Theft and Assumption Deterrence Act

Finally, the Identity Theft and Assumption Deterrence Act of 1998 is legislation designed specifically to combat identity theft. It provides for federal criminal penalties for individuals who possess, transfer, or produce fake identification. Although it enables victims of identity theft to receive help from federal law enforcement agencies, its weakness with regard to third party tort liability is that the law does not address the procedures used by identity thieves to gain access to confidential information. Additionally, the Act does not impose any obligations on financial institutions toward its customers and prospective clients.

**Conclusion**

Identity theft has become more and more common, both as the Internet has opened new avenues for access to personal data, and as financial institutions have increased their marketing efforts to win valuable market share. As more victimized consumers turn to those institutions for recourse, the courts — and possibly the legislature — will be called on to define the scope of the duties and obligations such institutions owe their customers as well as the public. The recent cases suggest that courts are willing to impose such duties on financial institutions and to enable consumers to recover damages. The coming years will show whether these initial warning signs are heeded by financial institutions, or whether victimized consumers will use the courts to force such institutions to change the practices that arguably facilitate these crimes.

ENDNOTES

3. See id.
5. See Higgins, supra note 4, at 43.
7. See id.
8. See id.
9 See Higgins, supra note 4, at 44-45; Millett, supra note 1, at 19.


11 See Suburban Trust Co. v. Waller, 408 A.2d758 (1979) (holding that bank depositor has right of confidentiality to all information and transactions relating to account).


13 Id. at 619.

14 Id. at 620.

15 681 So. 2d 1364 (Ala. 1996).

16 See id. at 1366.

17 Id. at 1365

18 See id. Patrick's ordeal shows the extent to which the theft of one's identity can reek havoc in a victim's life: As a result of the imposter's wrongdoing, eleven different jurisdictions issued arrest warrants for Patrick based on the bad checks written by the imposter. Patrick was taken into custody by five different jurisdictions for a total of ten days of incarceration while she attempted to prove her innocence and establish that her identity had been stolen. Id. at 1365-66. While it appears unlikely that Patrick was personally liable for any of the bounced checks, it seems perfectly clear that she nonetheless suffered "damages" as a result of the scheme.

19 See id. at 1368-69.


21 Id. at 1369.

22 Id.

23 Id.

24 See id. at 1370.

25 Id. at 1367.

26 Banks and financial institutions increasingly require unique passwords and "PINs" (personal identification numbers) to access or change data in an account. In addition, some institutions will seek to prevent account takeover by mailing a change of address notice to both the old and new address in conjunction with a request for an address change. See, e.g., California Public Interest Group, Theft of Identity: The Consumer X-Files (1996), at 20-21.

27 See id. at 1372.

28 15 USC § 6801.

29 See id. at § 6801(b).

30 See id. at §§ 6802, 6803.

31 15 USC § 1681.

32 See id. at § 1681(e).

33 225 F.3d 1063 (9th Cir. 2000).

34 See id. at 1065.

35 Id. at 1067.

36 Id.


38 18 USC § 1028.

© 2002 American Bar Association, Section of Litigation, All Rights Reserved. The Consumer and Personal Rights Newsletter is published at irregular
intervals by the Consumer and Personal Rights Litigation Committee of the American Bar Association’s Section of Litigation, 750 North Lake Shore Drive, Chicago, IL 60611. The views expressed in the Newsletter are those of the authors and do not necessarily reflect the position of the American Bar Association or the Section of Litigation. Comments and contributions to the Newsletter may be sent to Michael B. Hyman or the Committee Chairs.