

## **Identity Theft and Financial Institutions**

**By:**  
**Thomas P. Vartanian\***  
**Travis P. Nelson**

William Shakespeare, perhaps unknowingly, foretold the damage of identity theft: “But he that filches from me my good name/Robs me of that which not enriches him/And makes me poor indeed.”<sup>1</sup>

Back in 1969, words like “phishing,” “dumpster diving,” and “skimming,” or even “Internet” and “e-mail,” were not household terms, and “spam” was found in the grocery store. Yet it was in 1969 that U.S. Senator William Proxmire, author of the Fair Credit Reporting Act (“FCRA”), argued: “The consumer has a right to information which is accurate. He has a right to correct inaccurate or misleading information . . . . And he has the right to know when inaccurate information is entered into his file.” Thirty-seven years later, the importance of the consumer’s right to accurate information and the protection from those who would seek to threaten that right is among the forefront of national issues as put by President George W. Bush in February 2002: “One of the most harmful abuses of personal information is identity theft.”

Unlike crimes that involve a clear perpetrator and an obvious victim, identity theft harms both the individual whose identity has been stolen and the financial institution that unwittingly facilitated the fraudulent transaction. This article will examine the problem of identity theft and its impact on financial institutions and their customers, including the types of schemes that identity thieves perpetrate, and the financial and reputational consequences for financial institutions of such schemes.

---

<sup>1</sup> Othello, Act III, Scene 3.

“Identity theft” is a term that refers to a variety of crimes, all of which involve “stealing” someone’s personal identifying information.<sup>2</sup> An identity thief may use a variety of methods to obtain information, ranging from “basic street theft to sophisticated, organized crime schemes involving the use of computerized databases or the bribing of employees with access to personal information on customer or personnel records.”<sup>3</sup> Once an identity thief obtains the necessary information, he can assume the identity of the identity theft victim. The identity thief uses the information – and the victim’s reputation – to steal funds from the victim’s bank accounts, amass vast debts, or even commit crimes.<sup>4</sup>

Though exactly what acts constitute “identity theft” is as complicated and the variety of schemes that identity thieves perpetrate, patterns have evolved which allow for the following classifications: financial institutions fraud, credit card fraud, fraudulent loans, communications and utilities fraud, and others.<sup>5</sup> An identity thief’s fraudulent activities generally take one or both of two basic forms: “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

---

<sup>2</sup> S. Rep. No. 105-274, at 6 (1998).

<sup>3</sup> *Id.*

<sup>4</sup> U.S. Department of Justice, Identity Theft and Fraud, available at <http://www.usdoj.gov/criminal/fraud/idtheft.html> (last visited August 2, 2006) (on file with the authors).

<sup>5</sup> NACHA Internet Counsel, Internet Payments Fraud: A Primer for Merchants and Financial Institutions 14 (Feb. 3, 2003) at <http://internetcouncil.nacha.org/docs/Fraud%20Paper%20Final%20%20Jan%20%2703.pdf> (last visited August 2, 2006) (on file with the authors).

fraudulent charges).<sup>6</sup> Although criminal identity theft does occur, the vast majority of identity theft concerns white collar and financial fraud crimes.<sup>7</sup>

Identity theft can take many forms, however the Identity Theft Resource Center has identified several common schemes, for example:

- Visa/MasterCard Alert: A purported “employee” of a credit card issuer will call an unsuspecting customer trying to confirm unusual spending activity and ask for the security code on the back of the credit card.
- Phisher Scams: Identity thieves purchase a domain name that is similar to the domain name of a bona fide financial institution. For example, where the real website for a bank is “firstnationalbank.com” an identity thief will register “firstnationalbank-customerservice.com.” The thieves will then send out mass emails asking customers for verification purposes to supply their account information, social security number and other identifying information.<sup>8</sup>
- Dumpster Diving: Rummaging through trash bins, recycling containers and dumpsters to find credit card slips, ATM receipts, loan or credit card applications or bank statements.
- Change of Address: The thieves fraudulently request a change of address for credit card statements, then request additional cards, pre-approved credit offers, and other information.

---

<sup>6</sup> Nat’l White Collar Crime Center, WCC Issue: Identity Theft (Sept. 2002), available at <http://www.diogenesllc.com/identitytheft.pdf> (last visited August 2, 2006) (on file with the authors).

<sup>7</sup> U.S. Gen. Accounting Office, Identity Theft: Greater Awareness and Use of Existing Data Are Needed 3 (June 2002).

<sup>8</sup> The OCC has provided guidance for financial institutions on phishing deterrence, focusing on prevention, detection, and response. OCC Alert 2003-11, *Customer Identity Theft: E-Mail-Related Fraud Threats*, September 12, 2003.

- Spoofing: This is a method of creating fraudulent websites that look similar, if not identical, to an actual site, such as that of a bank. Customers are directed to these sites, and then lured into revealing confidential information that the identity thief will use to perpetrate the fraud, under the guise of legitimate banking business.<sup>9</sup>

Identity theft at financial institutions is caused by either carelessness in the handling of confidential customer information, or through intentional misconduct. Additionally, insiders at financial institutions use their access to confidential customer information to commit identity theft or aid and abet others in committing identity theft. In the past several years, the bank regulatory agencies have increased their efforts at combating these sorts of identity thieves through reviewing of previously filed suspicious activity reports (“SARs”). For example, the Office of the Comptroller of the Currency (“OCC”) reviews SAR reports for indications of identity theft, regardless of lost dollar amount, and then pursues such thieves under its “fast track” program.

In the late 1990’s, Congress took a substantial step toward deterring identity thieves through the Identity Theft and Assumption Deterrence Act of 1998 (the “Act”),<sup>10</sup> which specifically labels identity theft as a crime.<sup>11</sup> Prior to this Act, 18 U.S.C. § 1028(a) criminalized the unauthorized use or transfer of identity documents, such as a social security card, and 12 U.S.C. § 1029 criminalized the unauthorized use of credit cards, ATM codes, and similar information. The Act expanded the reach of these criminal statutes to include any person who

---

<sup>9</sup> OCC Alert 2005-24, *Threats from Fraudulent Bank Websites: Risk Mitigation and Response Guidance for Website Spoofing Incidents*, July 1, 2005.

<sup>10</sup> Pub. L. No. 105-318, 112 Stat. 3007 (amending 12 U.S.C. § 1028).

<sup>11</sup> 18 U.S.C. § 1028(a).

“knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law . . . .”<sup>12</sup> The law defines “means of identification” as including, among other things, social security numbers, dates of birth, unique biometric data, telecommunications identifying information, etc.<sup>13</sup> Most importantly, the Act recognized that criminals do not need the actual documents in order to harm their victims – “often they just need the information itself to facilitate these types of crimes.”<sup>14</sup> Further, with passage of this Act, the crime of identity theft was no longer viewed as merely a crime against the financial institution from which the information was compromised, but against the individual about whom the information related as well. This Act also required the Federal Trade Commission (“FTC”) to establish a central complaint system to receive and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus. There are a variety of other federal criminal statutes that are implicated by identity theft.<sup>15</sup>

In addition to criminal statutes, there are several other laws that impose duties on financial institutions to protect and monitor confidential customer information, such as the FCRA, the Gramm-Leach-Bliley Act (“GLBA”), and the USA PATRIOT Act. More recently, in 2003, President George W. Bush signed into law the Fair and Accurate Credit Transactions Act

---

<sup>12</sup> 18 U.S.C. § 1028(a)(7).

<sup>13</sup> *Id.* at § 1028(d)(3).

<sup>14</sup> S. Rep. No. 105-274, at 6.

<sup>15</sup> Identification Fraud, 18 U.S.C. § 1028; Credit Card Fraud, 18 U.S.C. § 1029; Computer Fraud, 18 U.S.C. § 1030; Mail Fraud, 18 U.S.C. § 1341; Wire Fraud, 18 U.S.C. § 1343; Mail Theft, 18 U.S.C. § 1708; Immigration Document Fraud, 18 U.S.C. § 1546; Financial Institution Fraud, 18 U.S.C. § 1344.

of 2003 (“FACT Act”).<sup>16</sup> The FACT Act permanently reauthorized the national uniformity provisions of the FCRA, and was a response to the growing reality that the increase in information sharing and growth in technology was in part a catalyst for identity theft. For example, the FACT Act added § 605A to the FCRA, establishing three instances where consumers can direct a nationwide consumer reporting agency to include a fraud alert in each consumer report furnished on those consumers.<sup>17</sup> These fraud alerts are designed to clearly and conspicuously notify users of consumer reports that the consumer may have been a victim of identity theft or other fraud. Through these fraud alerts, users of consumer reports are required to verify the identity of the consumer before establishing a new credit plan or loan obligation or issuing an additional card when requested by a consumer with an alert in his or her file.<sup>18</sup> The FACT Act requires a consumer reporting agency to place a fraud alert on a consumer’s credit file when requested by the consumer,<sup>19</sup> which then provides all prospective users of a consumer report on the consumer with a warning that the consumer does not authorize the establishment of any new credit plan or other new credit obligation in the consumer’s name, unless the user verifies the identity of the person making the request in an appropriate manner.<sup>20</sup>

The FACT Act further requires the banking agencies, the National Credit Union Administration (“NCUA”), and the FTC (collectively the “Agencies”) to jointly establish procedures for the identification of possible instances of identity theft – “red flag” guidelines and

---

<sup>16</sup> Pub. L. No. 108-159, 117 Stat. 1952 (2003).

<sup>17</sup> 15 U.S.C. § 1681c-1(a)(1)(A).

<sup>18</sup> 15 U.S.C. § 1681c-1(h)(1)(A).

<sup>19</sup> 15 U.S.C. § 1681c-1(a)-(b).

<sup>20</sup> 15 U.S.C. § 1681c-1(h)(1)(B)(i).

regulations.<sup>21</sup> The legislative history for this provision elucidates that this requirement was expected to result in the development of broad guidelines, thus resulting in policies and procedures that vary from institution to institution.<sup>22</sup> In July 2006, the Agencies offered proposed “red flags,” which the Agencies define as a pattern, practice, or specific activity that indicates the possible risk of identity theft.<sup>23</sup> The guidance addressed indicators of existing identity theft, as well as the possible existence thereof.<sup>24</sup> The guidance requires financial institutions to (i) design and implement identity theft programs, (ii) monitor on-going compliance with such programs, and (iii) establish “red flags” regarding possible consumer identify theft.

Under the proposal, financial institutions must have a written program that is based upon a risk assessment, which includes internal controls that address the identity theft risks identified through such assessment. Similar to the Agencies’ Information Security Standards, this program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities. It must also be flexible enough to address changing identity theft risks as they arise.

The program must include policies and procedures to prevent identity theft from occurring, including policies and procedures to:

---

<sup>21</sup> 15 U.S.C. § 1681m(e)(1)(A)-(B).

<sup>22</sup> S. Rep. No. 108-166, at 13 (2003).

<sup>23</sup> Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 71 Fed. Reg. 40786 (proposed July 18, 2006).

<sup>24</sup> It is this linkage between such events and identity theft that led the agencies to include the precursors of identity theft as among the red flags.

- Identify those red flags that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of the financial institution;
- Verify the identity of persons opening accounts;
- Detect the red flags that the financial institution identifies as relevant in connection with the opening of an account or any existing account;
- Assess whether the red flags detected evidence a risk of identity theft;
- Mitigate the risk of identity theft, commensurate with the degree of risk posed;
- Train staff to implement the program; and
- Oversee service provider arrangements.

The proposed regulation requires the board of directors of an institution, or an appropriate committee of the board, to approve the program. Further, the board, an appropriate committee, or senior management must exercise on-going oversight over the program's implementation, and staff implementing the program must report at least annually as to the program's compliance with the regulation.

The means to steal identities in an electronic information environment are varied and continually changing and increasing, so any "red flag" system must be regularly updated. The fact that many interfaces with the customer and much of the processing of electronic information and payments occurs through third party providers complicates the ability of any financial institution to completely control the implementation and execution of "red flag" systems.

In that regard, it should be clear that the regulation once adopted will establish a new standard of care. Consumers damaged by identity theft where the "red flag" system was not operable, up to date, effective or executed properly are likely to add a count to their complaints that the institution failed to comply with applicable standards of conduct required by law. This

will effectively provide consumers with a private right of action for an institution's failure to conform to the requirements of the final regulation.

As with the Bank Secrecy Act, identity theft legislation and regulations impose substantial compliance requirements on the financial services industry. The failure of such compliance programs to detect wrongdoing generates significant reputation, supervisory, and litigation risk. These guidelines, though deliberately drafted to provide flexibility so that institutions can implement programs that are most conducive to their unique needs, will likely form a basis by which the Agencies measure conformity with standards of safe and sound operation for enforcement purposes.

As stated, the promulgated regulatory standards of care for financial institutions' use of confidential customer information may lead to an increase in civil suits for such institutions' mishandling of customer information, as such regulations establish a baseline measurement for an institution's duty of care, a core element of any negligence complaint. Though it has met with mixed review in the courts, the common law tort of negligent enablement of imposter fraud remains a viable claim that may subject financial institutions to significant tort liability. Negligent enablement of imposter fraud is a narrowly framed cause of action that applies when the victim's identity theft losses result from a financial institution's negligence in assisting or furthering an identity thief's efforts at stealing the victim's identity.

The Supreme Court of Alabama, in *Patrick v. Union State Bank*, has upheld negligent enablement of imposter fraud where the imposter opened an account in the plaintiff/victim's name, and wrote several worthless checks.<sup>25</sup> The court notes that the "key factor" in such an

---

<sup>25</sup> *Patrick v. Union State Bank*, 681 So.2d 1364 (Ala. 1995).

action is foreseeability, as well as “the nature of the defendant’s activity; . . . the relationship between the parties; and . . . the type of injury or harm threatened.”<sup>26</sup> In upholding the duty that banks have to the public, the court noted:

Banks 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. Ordinary corporations handle their own money, but banks handle the money of other individuals. They are quasi-public corporations by nature, subject to regulation and supervision by the state.<sup>27</sup>

Conversely, the South Carolina Supreme Court rejected a negligent enablement of imposter fraud claim by a noncustomer plaintiff/victim who claimed that the defendant bank breached its duty in issuing credit cards to the identity thief imposter.<sup>28</sup> Citing a New York State Appellate Division decision, the South Carolina court rejected the plaintiff’s claim, noting “we . . . decline to recognize a legal duty of care between credit card issuers and those individuals whose identities may be stolen.<sup>29</sup> The relationship, if any, between credit card issuers and potential victims of identity theft is far too attenuated to rise to the level of a duty between them.” This decision is at odds with a previous South Carolina decision not mentioned in the case, *Murray v. Bank of America*, where an identity theft victim sued the bank that opened an

---

<sup>26</sup> *Id.* at 1368.

<sup>27</sup> *Id.* at 1368.

<sup>28</sup> *Huggins v. Citibank*, 585 S.E.2d 275 (S.C. 2003).

<sup>29</sup> *Id.* at 277, citing *Polzer v. TRW, Inc.*, 682 N.Y.S.2d 194 (N.Y. App. Div. 1998).

account for an imposter in her name.<sup>30</sup> The court determined that a relationship giving rise to a duty of care was created when the victim went to the bank and asked it to close the account opened by an imposter. The court took a somewhat unique position by concluding that, as one commenter explained it, the victim's "demand for a remedy created the duty that gave rise to the remedy."

Between these two approaches is a decision by the U.S. Court of Appeals for the Fourth Circuit in *Eisenberg v. Wachovia Bank, N.A.*,<sup>31</sup> where the court distinguished the stranger status of its victim from the status of the victim in *Patrick*. By emphasizing that the plaintiff had no cognizable relationship with the bank he sued, the *Eisenberg* court left open the possibility that a financial institution could owe a duty to an individual victimized by identity theft – particularly where the victim was a customer of the defendant. The *Eisenberg* court's approach is particularly relevant as several prominent banks have their home state within the Fourth Circuit's jurisdiction.

With the possibility that a special relationship may exist between a customer of a financial institution and that institution, there exists a growing likelihood that courts may allow suits for negligent enablement of imposter fraud to proceed past summary judgment. Further, with the FACT Act, and interagency guidelines on information security standards and identity theft prevention, courts may begin to recognize federal statutes and regulations as setting the standard of care for institutions to observe and by which they will be measured in tort suits.

The plague of identity theft has caused an increase in the responsibilities of chief privacy officers, whose role over the last decade has developed into that of a gatekeeper, protecting the

---

<sup>30</sup> 580 S.E.2d 194 (S.C. Ct. App. 2003).

<sup>31</sup> 301 F.3d 220 (4<sup>th</sup> Cir. 2002).

integrity of customer information, and monitoring its use by other institutional stakeholders, including third party providers. With the pressure of increased focus on financial institutions by federal regulators and plaintiffs' attorneys, financial institutions must make the prevention and deterrence of identity theft, and swift and open remediation of security breaches involving identity theft, a top priority.

---

Thomas P. Vartanian (Thomas.Vartanian@friedfrank.com) is a partner, and Travis P. Nelson (Travis.Nelson@friedfrank.com) is an associate, at the Washington, DC office of Fried, Frank, Harris, Shriver & Jacobson, LLP.