COMPLIANCE WITH THE NEW IDENTITY THEFT PREVENTION REGULATIONS

TIMOTHY L. MOHR AND RALPH M. FATIGATE

The proliferation of e-commerce and the simplification of Web site–creation technology has facilitated the escalation of identity theft, a crime that now affects millions of Americans and saps billions of dollars from U.S. businesses annually. Identity theft can affect a business's hard-won reputation and result in expensive litigation. New laws that go into effect on November 1, 2008, require banks and all other institutions that offer credit to protect themselves and their customers from identity theft in categorical ways. To comply with these regulations and avoid penalties resulting from audits by regulators, affected institutions must enact policies and procedures that identify red flags as described by the laws, detect them, and respond to them appropriately. Failure to comply with the new regulations on time can result in adverse regulatory actions.

The President's Task Force on Identity Theft, established by executive order on May 10, 2006, uses the Federal Trade Commission's definition of identity theft: "a fraud attempted or committed using identifying information of another person without authority."[1] The fraud now known as identity theft is not a new crime, but as financial transactions shifted toward electronic- and online-based technology, its capacity to wreak havoc has grown exponentially. The Federal Trade Commission ("FTC")

Timothy L. Mohr, CFE, MS, is a director in BDO Consulting's Investigations Practice. Ralph M. Fatigate is a director in BDO Consulting's Anti–Money Laundering Services Practice. He has lectured at the City University of New York Graduate Center on the subject of identity theft.

Published in the June 2008 issue of The Banking Law Journal.

estimates that 9 million Americans have their identities stolen every year. A 2003 FTC survey estimated personal and business losses to identity theft at $48 billion in the previous year.[2] That total has grown steadily ever since.

MECHANICS OF IDENTITY THEFT

As consumers and businesses have become more aware of the dangers of identity theft, thieves have become more sophisticated. Personal information and free credit card offers are still stolen from mailboxes. Scams that encourage unsuspecting job applicants to surrender their personal data in response to fake job offers also remain popular, as does the time-honored tradition of eavesdropping, or "shoulder-surfing." Dumpster divers can be foiled by paper shredders (although dogged criminals have been known to tape shredded documents back together). Online tactics, however, are now the preferred method for stealing data.

Phishing refers to attempts to persuade unsuspecting consumers to give up sensitive information, such as passwords or credit card numbers, by masquerading as a trustworthy entity, usually an online auction site, via a legitimate email complete with logos and working links to a Web site. The recipient is then threatened with the suspension or termination of his or her account for lack of compliance and is subsequently duped into "updating" a password or Social Security number. Armed with this information, thieves are able to steal money, credit, and even the account holder's identity.[3]

Pharming can result in a data security breach if a customer provides information related to his or her account to someone claiming to represent the financial institution or creditor via a fraudulent Web site, which is usually created to look exactly like that of the actual institution. Attackers generally access the giant databases that route Internet traffic. Real-time modifications divert users to the criminal sites before they access the intended ones.[4] Thieves choose large sites, ensuring that monitors of the legitimate servers never notice as the traffic diverted to the fake sites represent only a fraction of the typical volume.[5]

The simplification of Web site–building technology has put such scams within reach of more and more people. In 2004, for example, a German teenager hijacked the domain name eBay.com.de "just for fun." That time

the domain was returned without the commission of fraud.[6] Other instances have not ended as well and criminals always seem to stay one step ahead of software designed to foil phishing and pharming. Therefore, all companies that handle financial transactions over the Internet are at risk.[7]

The purposeful misdirection of personal mail is also often key to identity theft. Subsequently, would-be thieves also concentrate their efforts on the submission of fraudulent change-of-address requests to institutions that mail financial statements (or similar records containing sensitive information) to their customers. If successful, an identity thief can gather enough information to create chaos. For example, with only a bank statement, which contains an account number, information about total funds available, check numbers, and the bank's name (from which a routing number can easily be determined), a savvy criminal can wipe out the balance with new checks, printed with the old account number and a new, fake address. Misdirecting bank and credit card statements can also keep consumers from learning that their identities have been stolen until it is too late. For these reasons, managing and verifying change-of-address requests is a major part of the government's new anti-identity-theft Red Flag regulations.

NEW REGULATIONS

In response to an increase in identity theft, President George W. Bush signed the Fair and Accurate Credit Transaction Act ("FACT") into law on December 4, 2003. FACT added several new provisions to the Fair Credit Reporting Act of 1970, including enhancing the weapons consumers have in their arsenal for combating identity theft.

On October 31, 2007, the Federal Reserve, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, together with the U.S. Department of the Treasury and the Federal Trade Commission, took the next step and published a final set of Red Flag regulations that put certain sections of FACT into effect.[8] These regulations require all financial institutions and creditors to develop and implement written red flag identity theft programs no later than November 1, 2008. They also require credit and debit card issuers to establish policies

to assess the validity of all change of address requests.

The Red Flag rules are mandatory for all financial institutions, including banks, thrifts, mortgage lenders, and credit unions; casinos; U.S. branches, agencies, and commercial lending companies of foreign banks; and any other person or business arranging for the extension, renewal, or continuation of credit, including retailers, automobile dealers, utility companies, and telecommunications companies.

COVERED ACCOUNTS

The final rules differentiate between an *account*, an ongoing relationship between a person and a financial institution or creditor, including an extension of credit and a deposit account, and a *covered account*, an account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. Covered accounts also include any other account for which there is a reasonably foreseeable risk of identity theft, either to customers, the financial institution, or the creditor.

Financial institutions and creditors must periodically determine whether they offer or maintain covered accounts. Those that do must develop and implement written identity theft prevention programs to detect, prevent, and mitigate identity theft in connection with such accounts. These programs must be appropriate to the size and complexity of the institution and the nature and scope of its activities; they must also address the changing nature of identity theft risks. The development of these programs is not, therefore, a one-time event: it is a dynamic, ongoing process.

POLICIES AND PROCEDURES

An identity theft program must be risk based. Relevant red flags for covered accounts should be identified and incorporated into it. The program must then be able to detect any red flags that occur, respond to them appropriately, and ensure that the red flags themselves are updated periodically to reflect changes in identity theft risks to customers, the financial institution or creditor, and any service providers or vendors with which the institution

does business.

Written policies and procedures must be approved by the board of directors or an appropriate committee thereof. For a branch or agency of a foreign bank, the managing official in charge must give his or her approval; at a creditor without a board they must be approved by a management employee at the level of senior vice president or above. Lower-level employees may not oversee these programs.

The procedures must assign specific responsibilities for the program's implementation, for the approval of any material changes to the program, for the oversight of any arrangements with any services providers affected by the procedures, and for periodic reporting on (and the review of the reporting on) compliance with these regulations. These reports should evaluate how effectively the policies and procedures address the risk of identity theft with respect to both existing covered accounts and the opening of new ones. They should also cover any significant incidents involving identity theft, and management's response to them since the previous report, as well as any recommendations for material changes to the program.

Covered entities do not, however, have to create duplicate policies and procedures; existing procedures, controls, and processes can be used to address these requirements. For example, existing fraud prevention mechanisms might be leveraged to address these requirements.

Some questions to consider include: Do multiple business lines require a customized, enterprise-wide solution? Should customers be able to access their information only in person? What kind of accounts should customers be able to open online? The risk assessment conducted to assist in this determination should consider the following factors:

- Whether the regulations cover the accounts offered and maintained;
- The institution's size, location, and customer base;
- The methods it uses to open and access its accounts;
- The institution's previous experience with identity theft; and
- The cost and operational burden posed by countering any risk from identity theft.

Red Flags

Red flags are a pattern of specific activity that indicates the possible existence of identity theft. An entity can detect red flags by obtaining and verifying identifying information about a person opening a covered account by using the procedures regarding identification and verification set forth in the Customer Identification Program rules of the U.S. PATRIOT Act. These include policies for authenticating customers, monitoring transactions, and verifying the validity of change of address requests. (No specific technology, system, process, or methodology, however, is required.)

In identifying relevant red flags for covered accounts, an institution must consider the types of accounts it offers or maintains and how it opens and provides access to these accounts. Any previous experiences with or incidents of identity theft should be considered as potential red flags, as should methods of identity theft the financial institution or creditor has identified that reflect changes in risk level. Red flags for online transactions are likely to be different from those for face-to-face transactions.

Address Verification

The Red Flag rules' requirements for address verification, including e-mail addresses, are complex and are geared toward ensuring that institutions develop and implement policies and procedures making them reasonably confident that reports or statements they mail out or credit cards they issue actually belong to the consumers to whom they are sent. The rules also contain guidance for how to handle notices of address discrepancy sent by consumer reporting agencies. Existing customer identification procedures may be leveraged to meet the requirements of the new Red Flag regulations.

Updates

Program updates should reflect changes in risks to customers or to the financial institution's or creditor's security regarding identity theft. Such updates should consider any experiences the institution has had with identity theft since the program was last updated, changes in the types of accounts

the entity offers, as well as any recent mergers, acquisitions, alliances, joint ventures, or service provider arrangements. Methods of identity theft change continually, as do the technologies used to identify, mitigate, and prevent it; these developments must also be examined in relation to any risk assessment program.

Training

The procedures must include a training plan for the program's effective implementation. All existing employees must be trained in the aspects of the identity theft program in which they are expected to take part; the training must also be made part of any orientation program for new employees. Employees must be trained in any changes to the identity theft program in real time. In addition, the training program must include a mechanism to assess whether the training itself is relevant to the business and being delivered efficaciously.

Audits

The Red Flag rules require the establishment of control and audit guidelines in order to ensure that the program is implemented adequately and tested independently. Because audit frequency is based on risk, it will, at least initially, likely be more frequent in the program's initial stages.

RESPONDING TO IDENTITY THEFT

Once a red flag has been detected, the account involved should be monitored for evidence of identity theft. After the institution has made a determination of identity theft, it might take one or more of the following actions:

- Contact the customer;
- Change any passwords or security codes to the account;
- Temporarily freeze or close the account;

- Reopen the account with a new account number;
- Decline to open a new account; and
- Notify law enforcement and file a security assessment report.

The institution may also decide not to attempt to collect on the account or sell the account to a debt collector. Each triggering event is unique and must be reviewed individually. In some cases, a response may not be warranted if the impetus behind it is determined to be false.

BUSINESS MODEL CONSIDERATIONS

The incorporation of the policies and procedures required by the new Red Flag rules is likely to raise questions related to an institution's business model. Among the most pertinent are whether compliance will require an expansion in staffing and whether any compliance costs can — or should — be passed on to consumers. While these regulations will protect financial institutions and creditors from the massive costs of fraud, identity theft is a crime aimed at consumers, and the regulations were passed by Congress and signed into law with the public in mind. Should their introduction be made known to consumers, and in what way should consumers' expectations about them be managed? More importantly, will consumer groups feel that the regulations respond adequately to the threat?

CONCLUSION

Different organizations are tackling compliance with these regulations differently. Some are handling it through their fraud prevention departments; others, in their banking secrecy act departments; some in their credit risk areas; still others, in their consumer compliance departments.

A first step toward compliance might be to form a task force of all internal stakeholders and identify key senior members of management responsible for the timely development, implementation, and ongoing administration of the red flag identity theft program. The task force should review existing fraud prevention and customer identification policies and procedures to determine whether any can be leveraged to fulfill these new obliga-

tions. It should also assess whether the organization has the necessary resources in house to develop and document the program, or whether outside resources will be needed.

Any outside resources engaged should be able to develop a risk assessment methodology, define and develop the red flag identity theft program, conduct a review of a red flag program developed in house, author a training program and provide initial and ongoing employee training, and investigate and respond rapidly to any incidents of identity theft.

Banking regulators are already inquiring about the status of Red Flag regulation compliance programs. With only months to go, financial institutions, and creditors should take immediate measures to formulate their action plans in order to comply with the November 1 deadline.

NOTES

[1] Federal Trade Commission, "Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy," October 31, 2007. http://www.ftc.gov/opa/2007/10/redflag.shtm.

[2] Federal Trade Commission, *Identity Theft Survey Report* (prepared by Synovate), McLean, VA: 2003).

[3] Polly Samuels McLean and Michelle M. Young, "Phishing and Pharming and Trojans — Oh My!" *Utah Bar Journal*, April 2006. http://webster.utahbar.org/barjournal/2006/04/phishing_and_pharming_and_troj.html.

[4] Microsoft, "Pharming: Is Your Trusted Web Site a Clever Fake?" January 3, 2007. http://www.microsoft.com/protect/yourself/phishing/pharming.mspx.

[5] Jane Larson, "New Crop of Thieves: Pharmers Hit Net Banking," The Arizona Republic, April 19, 2005. http://www.azcentral.com/arizonarepublic/news/articles/0419pharming19.html#.

[6] Martin Fiutak, "Teenager Admits eBay Domain Hijack," C|net News.com, September 8, 2004. http://www.news.com/Teenager-admits-eBay-domain-hijack/2100-1029_3-5355785.html.

[7] Federal Deposit Insurance Corporation, *"Pharming": Guidance on How Financial Institutions Can Protect Against Pharming Attacks*, Financial Institution Letter FIL-64-2005. Washington, DC: July 18, 2005.

[8] Board of Governors of the Federal Reserve System, et al., "Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy," October 31, 2007. http://www.federalreserve.gov/newsevents/press/bcreg/20071031a.htm.