Final Federal Rules Require Identity Theft Prevention Programs to Be Implemented in 2008

JOHN L. NICHOLSON AND MEIGHAN E. O'REARDON

The authors discuss the new federal rules imposing identity theft-related requirements on financial institutions, creditors, credit and debit card issuers, and users of consumer credit reports, as well as guidelines and supplemental information also issued to assist affected entities.

Six federal agencies[1] have jointly issued final rules imposing identity theft-related requirements on financial institutions, creditors, credit and debit card issuers, and users of consumer credit reports (the "Rules"). The new regulations implement sections of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") and specifically call for:

1. Financial institutions and creditors to develop and implement a written "Identity Theft Prevention Program,"
2. Credit and debit card issuers to assess the validity of notifications of changes of address in conjunction with a request for a new card, and

John L. Nicholson is a senior associate in the Global Sourcing group of Pillsbury Winthrop Shaw Pittman LLP. He can be reached at john.nicholson@pillsburylaw.com. Meighan E. O'Reardon is an attorney at the firm.

Published in the January 2008 issue of Privacy & Data Security Law Journal.

3. Any user of consumer credit reports to implement reasonable policies and procedures when a consumer reporting agency sends a notice of address discrepancy.[2]

In addition to the final Rules, the lead federal agencies have issued guidelines and supplemental information to assist affected entities. These new Rules apply to any entity that extends credit, including financial institutions and small merchants. The final Rules became effective on January 1, 2008, and full compliance is required by November 1, 2008.

IDENTITY THEFT RED FLAGS AND ADDRESS DISCREPANCIES

On January 1, 2008, the Agencies' final Rules on Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 took effect.[3] The Rules implement Sections 114 and 315 of the Act, which specifically call for "establishment of procedures for the identification of possible instances of identity theft" and "reconciling addresses."[4] In addition to the new regulations, guidelines and supplemental information have been released to assist entities who must now implement specific identity theft policies and procedures during 2008.

The rules reflect the Agencies' final determinations.[5] The requirements across all six Agency versions are nearly identical, but there are some slight variations. Notably, the specific financial institutions affected by a particular Agency's regulation may vary.[6] As such, affected entities should consult the final language in the rule(s) specific to their regulator(s).

Three separate requirements focused on reducing identity theft are imposed by the regulations. The Rules specifically call for: (1) financial institutions and creditors to develop and implement a written "Identity Theft Prevention Program" to detect, prevent, and mitigate identity theft in connection with certain covered accounts, (2) credit and debit card issuers to assess the validity of notifications of changes of address in conjunction with a request for a new card, and (3) any user of consumer cred-

it reports to implement reasonable policies and procedures when a consumer reporting agency sends a notice of address discrepancy.[7]

Requirement 1 — Identity Theft Program

The most significant element of the new regulations requires financial institutions and creditors to establish a written Identity Theft Prevention Program ("Program") that is designed to "detect, prevent, and mitigate identity theft" in connection with specific accounts. Each entity's Program must be able to detect patterns, practices, and certain "red flag" activities that could signal possible identity theft. Red flags may include activity such as notification from a consumer reporting agency, suspicious account documents, suspicious personal identifying information, unusual use of a covered account, and warnings from customers.[8] Programs must include "reasonable policies and procedures" to:

1. Identify red flag activities for covered accounts and incorporate any newly identified red flag activities into the Program;
2. Detect red flag activities;
3. Respond to red flag activities that have been detected; and
4. Update the Program periodically to incorporate new risks.

It is crucial that each Program is dynamic and tailored to the financial institution's or creditor's particular business.

In addition to prescribing the necessary elements of the Program, the Rules also outline specific administrative requirements. These requirements identify the approvals, service provider oversight, and training to be associated with the Program. It is expected that members of the Board of Directors or appropriate senior management will participate in the development and implementation of the Program, and that members of the Board will ultimately approve the Program. According to the guidelines, annual reports to the Board or senior management should include assessments of the effectiveness of Program policies and procedures, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for material Program

changes. The Rules also require staff training to "effectively implement the Program."[9] The supplementary information released by the regulators note that this provision requires training of "relevant staff."[10] Staff training should vary by individual roles and degree of involvement with the Program. Training may be as fundamental as familiarizing certain staff with the new policies or more involved to include specific training and testing on the procedures to follow when a red flag is identified for a customer's account. Finally, financial institutions are expected to maintain appropriate oversight of applicable service-provider relationships.

Each entity's Identity Theft Prevention Program is only required to apply to specific customer accounts classified by the regulations as "covered accounts." According to the definitions within the red flag rules, such accounts primarily include personal accounts designed to permit multiple payments or transactions (*e.g.*, credit card accounts, mortgages, loans, etc.) and any account for which there is a foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. Defining the specific criteria for "covered accounts" should be an interactive process and involve analyzing how accounts are opened, how accounts are accessed, and the types of accounts most susceptible to identity theft. Under the Program, covered accounts must be periodically reassessed.

An important consideration for financial institutions and creditors when designing and implementing their Program is whether or not business accounts will be considered covered accounts. Business credit is increasingly becoming a target for theft. In February 2007, business executives' credit was targeted and used to open accounts in various small to midsized companies' names.[11] The identity thieves' tactic exploited the fact that business executives typically have good credit, that merchants are less likely to scrutinize business lines of credit, and that the merchant billing cycle to businesses can be as great as 60 days.[12] As such, in some instances it may be appropriate to incorporate business accounts into the Identity Theft Prevention Program, particularly when such accounts have previously been the target of identity theft. Factors to consider include the existing controls in place to protect business accounts, the level of risk posed by the business account (including the size, value, and method of

access), the number of individuals with access, and the types of transactions conducted through a particular business account.

Finally, entities should be aware that this requirement applies not only to large financial institutions but also to small merchants. Any business that extends credit, including finance companies, car dealers, or organizations that offer customers credit by signing for merchandise, must develop an Identity Theft Prevention Program.

Requirement 2 — Requests for Replacement Cards

The second element of the new regulations requires credit and debit card issuers to establish and implement reasonable policies and procedures to assess the validity of requests for a new or replacement card preceded by a change of address. Card issuers must verify address changes using the policies and procedures adopted as part of an Identity Theft Prevention Program, or by contacting the cardholder through the previous address on record and providing the cardholder a reasonable means of reporting an erroneous address change. Any notices sent to customers must be clear and conspicuous and separate from monthly account statements. This requirement is triggered by all types of address change notices including those directly from the customer, the post office, and return receipts. Finally, card issuers are permitted to assess the legitimacy of the address change either at the time the change request is made or when additional cards are requested. This rule is aimed at detecting and stopping a common tactic used by identity thieves.

Requirement 3 — Address Discrepancies

The final requirement is directed at users of consumer credit reports and applies whenever a notice of an address discrepancy is received from a credit reporting agency. Users of consumer credit reports include any person or entity that either uses or requests the report. Notably this requirement does not apply to a financial institution or creditor that does not use consumer credit reports.[13] All users of such credit reports must have policies and procedures in place to be able to form a "reasonable belief" that the consumer credit report relates to the specific individual in question. The Rules note that reasonable policies may include comparing

the information in the consumer credit report with information the user obtains and uses as part of its existing "Customer Identification Program" or acquires from third-party sources. Verifying the correct address directly with the customer is also an option. Additionally, in an effort to improve consumer credit reporting data, users that have confirmed the correct address, maintain a continuing relationship with the consumer, and regularly furnish information to the credit reporting agency that supplied the questionable address are required to communicate the confirmed address to the credit reporting agency.

KEY COMPLIANCE DATES

The new Rules took effect on January 1, 2008. Affected entities have 10 months to review current practices, develop security programs, and implement the necessary changes before full compliance is expected by November 1, 2008.

DESIGN AND IMPLEMENTATION—WHAT TO DO IN 2008?

These new Rules are broad and may overlap with existing programs and practices. As such, both large and small entities are likely to face challenges implementing the new identity theft regulations. Small and midsized institutions will likely need to build out new processes to address these requirements, and in some instances may need to develop additional identity theft expertise. Larger institutions, however, are likely to face difficulties locating the appropriate stakeholders who can effectively design and implement the Program. At a minimum, both types of entities should assemble an interdisciplinary team of individuals to develop the mandated policies and procedures. Expertise from the organization's business team, legal and compliance department, information technology group, fraud specialists, as well as other offices with identify theft experience, will be necessary.

Each entity required to implement the new Rules should start its compliance efforts by acquiring high-level organizational support. Buy-in and support from the Board of Directors and senior management is a crucial first step, especially given the need for their ongoing oversight and ulti-

mate approval of the Program. Organizations should also consider proceeding by identifying gaps between and overlaps with existing programs and the new regulatory requirements and conducting a risk assessment of active customer accounts. The necessary activities will vary for each organization and will depend in large part on the organization's existing fraud detection and compliance programs and experience with identity theft.

NOTES

[1] The Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Federal Trade Commission, and the Department of Treasury's Office of the Comptroller of the Currency and Office of Thrift Supervision (the "Agencies").

[2] *See* Federal Register, Vol. 72, No. 217, Friday November 9, 2007 at 63718.

[3] *Id.*

[4] Pub.L. 108-159 §§ 114, 315 (2003).

[5] The regulations specific to each Agency can be found as follows: Department of Treasury Office of the Comptroller of the Currency at 12 CFR Part 41; the Federal Reserve System at 12 CFR Part 222; the Federal Deposit Insurance Corporation at 12 CFR Parts 334 and 336; the Department of Treasury Office of Thrift Supervision at 12 CFR Part 571; the National Credit Union Administration at 12 CFR Part 717; and the Federal Trade Commission at 12 CFR Part 681.

[6] For example, the FDIC Red Flag regulation applies to "a financial institution or creditor that is an insured state nonmember bank, insured state licensed branch of a foreign bank, or a subsidiary of such entities (except brokers, dealers, persons providing insurance, investment companies, and investment advisors)" whereas the National Credit Union Administration's Red Flag regulation applies to "a financial institution and creditor that is a federal credit union."

[7] *See* Federal Register, Vol. 72, No. 217, Friday November 9, 2007 at 63718.

[8] The guideline supplement includes an illustrative list of 26 different types of red flags that financial institutions and creditors may consider incorporating into their Program.

[9] 12 CFR Part 41.90(e)(3), 12 CFR Part 222.90(e)(3), 12 CFR Parts 334.90(e)(3), 12 CFR Part 571.90(e)(3), 12 CFR Part 717.90(e)(3), and 12

CFR Part 681.2(e)(3).

[10] *See* Federal Register, Vol. 72, No. 217, Friday November 9, 2007 at 63731.

[11] Larry Greenemeier, "Latest Identity Theft Scam Targets Business Executives," Information Week (Feb. 15, 2007). See http://www.informationweek.com/news/showArticle.jhtml?articleID=197006538.

[12] *Id.*

[13] *See* Federal Register, Vol. 72, No. 217, Friday November 9, 2007 at 63735.

[14] Banks, thrifts, and credit unions, and certain non-federally regulated banks, are required to have customer identification programs in accordance with 31 CFR Part 103.121, which implements Section 326 of the USA PATRIOT Act.