Spring, 2009

PENNSYLVANIA BAR ASSOCIATION
Your Other Partner

Business Law Section NEWSLETTER

Chair: John B. Lampi
Editors: Louis F. Del Duca and Paula A. Schmeck

TABLE OF CONTENTS ...

continued on next page

FROM THE CHAIR ...

Greetings from the Business Law Section!

Members of the Business Law Section are currently working with the legislative staff of the PBA as well as staff from the General Assembly in preparing a number of pieces of legislation for introduction in this session of the General Assembly. Some of this legislation will need to go through the review and approval process of the PBA before formal introduction by members of the General Assembly for enactment. However, the amendments to the Business Corporation Law and other laws governing business entities which did not get through the General Assembly last session will be reintroduced in this session. We will keep all of our members informed on the progress of this business-law oriented legislation through the PBA's legislative staff's news e-mails to PBA members.

John B. Lampi

Your Business Law Section's committees monitor other bills that are introduced by members of the General Assembly to assist the PBA on whether or not to take a position on such legislation. Our Business Law Section committees offer you experience in this aspect of "lawyering". It is a great way to become knowledgeable about an area of the law in which you may have an interest. Please contact any of the Business Law Section officers or committee chairs if you are interested in participating in committee work.

Our broader Business Law Section Council meets periodically through telephone conferences. Our Business Law Section Council meetings for the first half of 2009 are at

continued on page 2

TABLE OF CONTENTS ...

FROM THE CHAIR ...

continued from page 1

noon, on Wednesdays, February 11 and April 8. You, as a member of the Business Law Section are invited to participate. We have a toll-free telephone conference system available to you or you can meet at the offices of one of our Council members to participate in person. We urge you to participate in our Council meetings.

Finally, we will hold our annual meeting of the Business Law Section in conjunction with the PBA Annual Meeting in Pittsburgh on June 3, 2009. If you are attending the PBA Annual Meeting, stop by and attend the Business Law Section annual meeting.

Please feel free to contact me if our Business Law Section can be of assistance in your practice. My telephone and e-mail information is (717) 243-6222 or jlampi@sfl-law.com.

Cordially,

John B. Lampi, Chair

This article, published in the Spring 2009 Business Law Section Newsletter, appears here with permission from the Pennsylvania Bar Association.

PENNSYLVANIA BAR ASSOCIATION

Your Other Partner

RED FLAG RULES REQUIRE COMPANIES TO TAKE IDENTITY THEFT SERIOUSLY

You may be surprised to that learn your business must comply with the new identity theft Red Flag Rules. Not only are credit card companies and financial institutions subject to these rules, but any company that regularly extends or merely arranges for the extension of credit is also subject to the rules. Thus, finance companies, mortgage brokers, automobile dealers, telecommunications companies, and utility companies, among others, will have to comply with the Red Flag Rules. If your company extends or arranges for the extension of credit, it had only until November 1, 2008, to become compliant with the Red Flag Rules.

Background

On December 4, 2003, the President signed into law the Fair and Accurate Credit Transactions Act ("FACTA"). FACTA was enacted by Congress to provide consumers with increased protection from identity theft. The regulations directed six agencies to jointly "establish and maintain guidelines…[that] identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft."[1] Accordingly, the six agencies published the final regulations on November 9, 2007, and those regulations was effective January 1, 2008.[2] However, compliance with the regulations is not mandatory until November 1, 2008.[3]

The final regulations contain three parts. First, they require covered entities to create a written identity theft program designed to detect, prevent, and mitigate identity theft in connection with certain covered accounts (the "Red Flag Rules" or the "Rules"). Second, the regulations impose requirements on consumer reporting agencies related to discrepancies between an address contained in a request for a consumer report and the address in the consumer reporting agency's file. Third, the regulations impose requirements on debit and credit card issuers to implement procedures to assess the validity of address changes under certain circumstances. This Commentary focuses on only the Red Flag Rules portion of the regulations.

Covered Entities

The Red Flag Rules cover "financial institutions" and "creditors" that offer or maintain "covered accounts." The breadth of the Rules comes from the broad definition of creditors. The term "creditor" means "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."[4] Consequently, many entities involved in the process of extending or maintaining credit must comply with the Red Flag Rules despite the fact that they do not extend credit themselves. For example, a retailer that takes applications for a third-party credit card or the car dealer that partners with a local bank branch to facilitate car loans will likely be subject to the Rules. Similarly, where nonprofit and government entities, such as many hospitals, defer payment for goods and services, they too will be considered creditors.

In addition to creditors, financial institutions are also required to comply with the Red Flag Rules. For purposes of the Rules, "financial institution" means banks, savings and loan associations, mutual savings banks, credit unions, or any other person who, directly or indirectly, holds a transaction account belonging to a consumer.[5]

Under the Red Flag Rules, only those creditors and financial institutions that offer or maintain covered accounts are required to develop and implement an identity theft prevention program. A "covered account" is "(i) [a]n account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions…and (ii) any other account…for which there is a reasonably foreseeable risk to customers…from identity theft…."[6] Covered accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, and checking and savings accounts. In determining whether the Red Flag Rules apply, a company should consider the types of accounts it offers, the methods it provides to open its accounts, the methods it provides to access its accounts, and its

continued on next page

previous experiences with identity theft.[7] Additionally, the company should periodically perform a reassessment of all of its accounts to determine whether they are covered accounts that trigger the application of the Rules.

Designing a Program

Companies subject to the Red Flag Rules must design and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.[8] The Rules do not specify the contents of the program that must be adopted. They give companies a lot of flexibility and merely require that a company design and implement a program that is appropriate to the size and complexity of the company and the nature and scope of its activities.

The Red Flag Rules do require identity theft prevention programs to include "reasonable policies and procedures" to identify relevant red flags and incorporate them into the program, to detect those red flags, to respond appropriately when red flags are detected, and to ensure that the program is updated periodically. Each of these elements is discussed below.

Identify Relevant Red Flags. The first element in the identity theft prevention program, as required by the Red Flag Rules, is to determine which red flags are relevant to the company and incorporate those red flags into its program.[9] "Red flags" are patterns, practices, or specific activities that indicate the possible existence of identity theft in connection with a covered account. The company should examine the covered accounts it currently offers or maintains and identify potential sources of red flags. The Rules include a set of guidelines that must be considered in implementing a program and set forth 26 examples of potential red flags. While not all 26 of the example red flags must be incorporated, the company should seriously consider each and have legitimate reasons for not incorporating any of them in the final written program. The company should also take into account its previous experience with identity theft in determining the appropriate red flags for its program. Some examples of red flags include:

- an application appears to have been forged, altered, or destroyed and reassembled;
- a consumer report includes a fraud alert, credit freeze, or address discrepancy;
- a change of address notice is followed shortly by a request for a new credit card, bank card, or cell phone;
- the Social Security number supplied by an applicant is the same as that submitted by another person opening an account;
- the address or telephone number supplied by an applicant is the same or similar to the account number or telephone number submitted by an unusually large number of other persons;
- the financial institution or creditor is notified that the customer is not receiving account statements;
- and an account that has been inactive for a reasonably lengthy period of time is used.

Detect Red Flags. The company should implement procedures to detect the identified red flags. The company should be sure to verify the identity of persons opening new covered accounts and should authenticate customers with existing covered accounts.[10] The company can refer to the verification procedures set forth in the Customer Identification Program rules that apply to financial institutions for guidance.[11]

Establish Response Procedures. The company should develop appropriate policies and procedures to respond to any red flags that are detected. The response should be commensurate with the degree of risk posed, which may include monitoring an account, contacting the customer, changing passwords, or notifying law enforcement. In some situations, it may be appropriate to determine that no response is necessary.[12]

Ensure the Program is Updated Periodically. It is important for the company to periodically update its program to reflect changes in risks. The company must

continued on next page

keep current with changes in identity theft and, as necessary, utilize new methods of combating identity theft. Additionally, the company should be aware that risks may change when it alters its business arrangements or modifies the types of accounts it offers.[13]

Methods for Administering the Program

Approval of the initial written program must be obtained from the company's board of directors or an appropriate committee thereof.[14] Oversight of the implementation of the program must be done by the board, a board committee, or a designated employee at the level of senior management.[15] This oversight also includes reviewing reports and approving material changes to the program.[16] If the company has any arrangements with service providers, it must ensure that any service provider's activity with regard to covered accounts is performed in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.[17]

Consequences of Noncompliance

Failure to comply with the Red Flag Rules can result in various penalties. Consequences may include a civil money penalty for each violation, regulatory enforcement action, and negative publicity.[18] Although the Rules do not allow for any private legal action,[19] there is the potential for private plaintiff lawsuits because a violation of federal rules may itself be a violation of state laws. These state laws may permit actions by consumers or state attorneys general. In any event, it is likely that, over time, the Red Flag Rules will become a de facto standard of care applied to determine whether a company has negligently caused a customer's identity to be stolen.

Conclusion

In general, the new Red Flag Rules require companies with covered accounts to take reasonable measures to ensure the safety of sensitive consumer information. The Rules are intended to detect, prevent, and mitigate the risk of identity theft, but they do not require companies to adopt any particular policy or procedure. Rather, companies can scale their programs to match the size, complexity, and nature of their businesses. The process a company follows in adopting its identity theft prevention program will go a long way toward establishing that the program is reasonable. At a minimum, a company should be capable of justifying the policies and procedures it adopts by demonstrating it has seriously considered the pertinent risks and has attempted to minimize them.

Kevin D. Lyles
Jones Day

(Footnotes)

1 15 U.S.C. § 1681m(e)(1)(A) & (2)(A). The six agencies responsible for issuing the joint guidelines are as follows: (1) the Office of the Comptroller of the Currency, Treasury; (2) the Board of Governors of the Federal Reserve System; (3) the Federal Deposit Insurance Corporation; (4) the Office of Thrift Supervision, Treasury; (5) the National Credit Union Administration; and (6) the Federal Trade Commission.
2 Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transaction Act of 2003; Final Rule, 72 Fed. Reg. 63718 (to be codified at 12 C.F.R. pts. 41, 222, 333, 364, 571, and 717 and 16 C.F.R. pt. 681). Note that each of the six agencies will codify the regulations at different parts. For simplicity, all future general references to the regulations will be cited to the Office of the Comptroller of the Currency's codification at pt. 41.
3 Id.
4 15 U.S.C. § 1691a(e).
5 15 U.S.C. § 1681a(t).
6 72 Fed. Reg. 63718, 63753–63754 (to be codified at 12 C.F.R. 41.90(b)(3)(i) and (ii)).
7 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(c)(1) through (3)); Appendix J to Part 41 II(a)(1) through (4).
8 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(d)(1)).
9 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(d)(2)(i)).
10 Appendix J to Part 41 III(a) and (b).
11 31 U.S.C. 5318(l) (31 C.F.R. 103.121).
12 Appendix J to Part 41 IV(a), (b), (c), (h), and (i).
13 Appendix J to Part 41 V(d) and (e).
14 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(e)(1)).
15 72 Fed. Reg. 63718, 63754 (to be codified at 12 C.F.R. 41.90(e)(2)).
16 Appendix J to Part 41 VI(a)(2) and (3).
17 Appendix J to Part 41 VI(c).
18 Press Release, Reuters, "Compliance Coach Identifies 23 New Identity Theft Red Flags Based on Recent Cases" (May 5, 2008) (http://www.reuters.com/article/pressRelease/idUS97072+05-May-2008+BW20080505) (last visited November 11, 2008).
19 Plaintiffs have attempted to bring private actions under the Fair Credit Reporting Act (15 U.S.C. § 1681m) because of an apparent drafting error in § 1681m(h)(8). Courts have differed on

continued on next page

the interpretation of the drafting error. Most recently, the United States Court of Appeals for the Seventh Circuit refused to permit such actions, ruling that the newly added § 1681m(h)(8) was designed to preclude private enforcement of the entirety of § 1681m, not just § 1681m(h). Perry v. First National Bank, *459 F.3d 816 (7th Cir. 2006). But see* Barnette v. Brook Road, Inc., *429 F. Supp. 2d 741 (E.D. Va. 2006).*