EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *November 2010*

The FTC's Red Flags Rule on Identity Theft Protection Will Be Effective December 31, 2010

The FTC "Red Flags Rule" mandating identity theft protection programs for financial institutions and a broad range of other companies will go into effect December 31, 2010. Red Flags are warning signals that should alert a business to the risk of identity theft.

Theodore P. Augustinos
Partner

Barry J. Bendes, Partner

Mark E. Schreiber, Partner

Socheth Sor, Associate

While prior deadlines have been extended, companies should be prepared that this time enforcement will go into effect. If you are covered by the Rule, you must adopt effective programs to identify Red Flags and detect, mitigate and deal with identity thefts when they occur. This may require changes to your computer, information security, and/or privacy policies.

What is the Red Flags Rule?

The Rule (16 CFR 681) requires "financial institutions" and "creditors" with "covered accounts," as defined under the Rule and discussed below, to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft. The program must be approved by the company's board of directors (or its highest governing authority), an appropriate committee designated by the board, or a designated employee at the level of senior management if a company does not have a board of directors.

First, companies need to determine whether they are subject to the Rule. Then, if they are, they must adopt and enforce an effective Red Flags Identity Theft Prevention Program before December 31. Traditional financial institutions (such as banks) regulated by the federal financial institutions regulatory agencies were required to comply with the Rule by November 28, 2008.

The new effective date does not affect financial institutions, but will impact a significant number of other companies that may not realize they are now subject to FTC regulation. Even companies that may be in compliance with the Massachusetts information security regulations (201 CMR 17.00), HIPAA, and other federal or state data security requirements will need to analyze the applicability of the Rule and adjust existing policies and procedures accordingly.

Does Your Company Need to Comply?

Financial Institutions

For purpose of the Rule, "financial institution" is defined as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person that, directly or indirectly, holds a transaction account . . . belonging to a consumer." 15 USC §1681a(t).

"Creditor" Has a Broad Definition.

If you meet the broad definition of "creditor" and also have "covered accounts," you are now subject to the Rule. The term "creditor" is expansively defined to mean "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 participate in the decision to extend, renew or continue credit." 15 USC §1681a(r)(5). For this purpose, a person includes a business, not-for-profit entity or other entity. The breadth of the definition has caused concern that the Rule reaches entities other than traditional financial institutions or creditors that engage in regular loans or advances. For example, it would appear to cover any entity that extends credit, gives credit terms (such

as permitting payment at the end of the month for goods or services rendered) or forbears in the collection of debts or bills, permitting multiple or extended payments.

This would include not only retailers, but also professional service providers and others. The FTC explained in a letter to the American Medical Association ("AMA") that the definition of "creditor" is not industry-based; rather, it is activity-based. In other words, whether a company qualifies as a creditor depends on how it accepts payment from its customers, not on the type of company it is or the services it provides. Thus, any entity that permits deferred payments (such as 30 days net) may be a "creditor" for purposes of the Rule, according to the FTC. Many arrangements in which a bill is issued but payment is subsequent to the provision of goods and services are viewed as providing an extension of credit.

Do You Have a "Covered Account?"

A company is subject to the Rule if it is a creditor (or a financial institution) that has "covered accounts."

The Rule defines two types of "covered accounts." First, a covered account is an account offered primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions. These types of accounts include utility, cell phone, mortgage, car loan, credit card and various accounts too numerous to list here.

Second, "covered account" is defined to mean any other account, including business accounts ("B to B" accounts), that the company offers or maintains for which there is a reasonably foreseeable risk to consumers or to the safety and soundness of the company from identity theft. Therefore, an account that does not meet the first part of the definition may still be a covered account if it poses a reasonably foreseeable risk of identity theft. Each company that meets the definition of "creditor" must do the analysis to determine whether it has "covered accounts." If so, the company must comply with the Rule.

Application of the Red Flags Rule

The Rule is designed to be risk-based and to take into account the burden that the Rule could impose upon an entity that has only a small risk of identity theft. Higher-risk entities need to have more comprehensive Identity Theft Prevention Programs. Lower risk entities are permitted to have a less robust program. However, all creditors that have covered accounts are required to establish, test and employ an effective program to identify and act upon "red flags" alerting the company of identity theft or the potential for identity theft and actual incidents of identity theft that come to its attention. Just having a program is not enough. The program must be flexible, adaptive and effectively enforced.

The Rule is designed to be risk-based and to take into account the burden that the Rule could impose upon an entity that has only a small risk of identity theft.

Are There Any Industry Exemptions?

The FTC has not identified any exempt industries. The American Bar Association ("ABA"), the American Institute of Certified Public Accountants ("AICPA"), and the AMA have brought lawsuits to prevent the FTC from enforcing the Rule against their members. For now, attorneys, doctors and accountants are not subject to the Rule, but until it is resolved by the courts, the reprieve is only temporary. Oral argument for the ABA lawsuit, originally brought in the U.S. District Court for the District of Columbia, is now scheduled for November 15, 2010 in the D.C. Court of Appeals. Both the AMA and AICPA have submitted amicus briefs in support of the ABA position.

The House of Representatives approved a bill to exempt legal as well as health care and accounting practices with 20 or fewer employees from the Rule. A parallel bill is pending before the Senate Committee on Banking, Housing and Urban Affairs. If the bills are enacted and signed into law, only legal, accounting, and healthcare practices with fewer than 20 employees would be exempt and those with more than 20 employees that meet the definition of "financial institutions" or "creditors" that maintain "covered accounts" would still be required to comply with the Red Flags Rule by December 31, 2010, unless the courts rule otherwise.

Penalties for Non-Compliance

Civil penalties of up to $3,500 per violation may be assessed, and injunctive relief as well as additional legal exposures in the event of a breach and resultant lawsuits can be anticipated. According to the FTC,

each instance in which a company violates the Rule is considered to be a separate violation. "Stacking" of penalties is not uncommon, for instance, where multiple infractions or numerous individuals had their data breached or identities stolen due to inadequate security practices.

What You Need to Do to Comply with the Red Flags Rule

Each business or individual must:

- Establish whether it is subject to the Rule by determining if it is a financial institution or "creditor" maintaining covered accounts.
- Determine if its business nevertheless presents a reasonable foreseeable risk of identity theft.

If either of the above applies, then, the following steps should be taken before December 31:

- Identify the Red Flags (warning signs) that would alert it to the possibility of identity theft;
- Set up procedures to detect these Red Flags by developing an effective written Identity Theft Prevention Program;
- Coordinate adoption and periodic review of the program by the board of directors, governing body or other senior level management authority, if there is no board of directors; and
- Implement the program by providing appropriate training to staff.

Additional Resources

The FTC maintains a Red Flags micro-website that has practical resources to assist companies with compliance. The FTC has published a helpful list of frequently asked questions, a "Do-It-Yourself" Red Flags program for entities that are at low risk for identify theft, a How-To Guide for Businesses and a short video on this website, all of which are available at http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml.

Conclusion

The Red Flags Rule is just one of a number of requirements designed to prevent identity theft. Doubtlessly, there will be more legislation and compliance follow-up required, both at the state and federal levels.

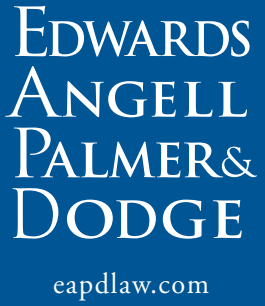
Each business or individual must:

- *Establish whether it is subject to the Rule by determining if it is a financial institution or "creditor" maintaining covered accounts.*
- *Determine if its business nevertheless presents a reasonable foreseeable risk of identity theft.*

Boston MA | Ft. Lauderdale FL | Hartford CT | Madison NJ | New York NY | Newport Beach CA | Providence RI
Stamford CT | Washington DC | West Palm Beach FL | Wilmington DE | London UK | Hong Kong (associated office)

This advisory is for guidance only and is not intended to be a substitute for specific legal advice. If you would like further information, please contact the Edwards Angell Palmer & Dodge LLP attorney responsible for your matters or one of the attorneys in the Privacy and Data Protection Group listed below:

Mark E. Schreiber, Partner, Chair	+1 617 239 0585	mschreiber@eapdlaw.com
Theodore P. Augustinos, Partner, Co-chair	+1 860 541 7710	taugustinos@eapdlaw.com
Laurie A. Kamaiko, Partner, Co-chair	+1 212 912 2768	lkamaiko@eapdlaw.com
Barry J. Bendes, Partner	+1 212 912 2911	bbendes@eapdlaw.com
Socheth Sor, Associate	+1 860 541 7773	ssor@eapdlaw.com



eapdlaw.com