

## Client Advisory | November 2009

# Recent Developments: The FTC Red Flags Rule and Massachusetts Security Regulation

October 30, 2009 brought several noteworthy developments to the enforcement of the Red Flags Rule and finalization of the Massachusetts security regulation, all of which may affect what you must do to comply.



Mark E. Schreiber, Partner



Theodore P. Augustinos  
Partner



Barry J. Bendes, Partner



Socheth Sor, Associate

The FTC extended the enforcement date of the Red Flags Rule as it applies to non-financial institutions from November 1, 2009 to June 1, 2010. The extension came at the request of several members of Congress following the unanimous approval of HR 3763 on October 20, 2009, a bill that, if adopted and signed by President Obama, would exempt health care, legal and accounting practices with *fewer than 20 employees* from the Red Flags Rule. The FTC agreed to the delay to allow Congress to finalize the legislation and to ensure that it does not begin to enforce a regulation that Congress plans to supersede.

Judge Reggie B. Walton of the D.C. federal court issued an order granting an injunction prohibiting the Federal Trade Commission (“FTC”) from enforcing the Red Flags Rule against attorneys. Judge Walton ruled from the bench stating that he had trouble accepting the FTC’s definition of creditor. In the formal opinion that followed, Judge Walton stated that the application of the Red Flags Rule to attorneys exceeds the FTC’s statutory authority under the Fair and Accurate Credit Transactions Act of 2003. The ruling may be only a temporary reprieve as appeal from the FTC is anticipated.

The Massachusetts Office of Consumer Affairs and Business Regulation filed its final amendment to the Massachusetts security regulation (the “Regulation”) (effective date is March 1, 2010).

### Red Flags Rule: Who Must Comply

The Red Flags Rule (16 CFR 681.1) requires that “financial institutions” and “creditors” with “covered accounts,” as defined under the Red Flags Rule, develop and implement a

written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft. For financial institutions, compliance has been required since November 28, 2008. As noted above, for institutions under the jurisdiction of the FTC, the Red Flags Rule are not effective until June 1, 2010.

### “Creditor” Used Broadly

The term “creditor” is broadly 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(i)(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 Red Flags Rule reaches entities other than traditional financial institutions or creditors that engage in regular loans or advances. It seems also to cover forbearance in the collection of debts or bills or persons permitting multiple or extended payments.

The Red Flags Rule is not industry-based, but rather it is activity-based. It does not focus on the type of company or the services provided. Whether a company qualifies as a creditor will depend on its terms of sale or service and how it demands payment from its customers. In its Frequently Asked Questions, the FTC has stated that the term creditor is broad and includes businesses or organizations that regularly provide goods or services first and allow customers to pay later. Many businesses bill after a sale is completed or services are provided. In the view of the FTC, this is a covered extension

of credit requiring compliance with the Red Flags Rule. Thus, individuals and entities providing deferred or extended payments are considered “creditors” under the FTC’s interpretation.

Although there were no intended exemptions from the Red Flags Rule, given the new developments in the last week, for now, attorneys are exempt from enforcement at least for the moment while the federal court injunction is in effect. Subject to the passage of HR 3763, certain businesses with less than 20 employees may also be exempt.

### Do You Have a “Covered Account?”

To be subject to the Red Flags Rule, not only must you be a creditor, but you must also have covered accounts.

The Red Flags Rule define “covered accounts” in two parts. First, a covered account is one that is 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, checking/saving, cell phone, mortgage, car loan, credit card accounts. The second kind of “covered accounts” is any other account 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.

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

**By the time the Red Flags Rule goes in to effect, each covered person (business or individual) must:**

1. Establish whether it is subject to the Rule by determining if it is a financial institution or “creditor.”
2. If it is a covered financial institution or creditor, it must determine if it maintains covered accounts.
3. If the answers to the above questions are “No,” then the person is not subject to the Red Flags Rule (but may have other obligations to its constituencies).
4. If the answers to Questions 1 and 2 are “Yes,” then,

- a. The person must identify the Red Flags (warning signs) that would alert it to the possibility of identity theft.
- b. Set up procedures to detect these Red Flags by developing an effective written Identity Theft Prevention Program.
- c. The board of directors, governing body or other senior level management authority, if you do not have a board of directors, must adopt the program and review it periodically.
- d. Implement the program by providing appropriate training to staff.

### Application of the Red Flags Rule

Even though the enforcement date of the Red Flags Rule has been delayed, it is important for a number of reasons for every business to start to put appropriate processes and procedures in place to identify warning signs of identity theft and to act accordingly when triggers are identified whether or not the Red Flags Rule goes into effect.

The Red Flags Rule is designed to be risk-based and to take into account the burden that the Red Flags Rule could impose upon an entity that has only a small risk of identity theft. The FTC makes clear that higher-risk entities need to have more comprehensive Identity Theft Prevention Programs. Lower risk entities are permitted to have a less complex program. However, all covered persons are required to establish, test and employ an effective program to identify and act upon “red warning flags” alerting the person of identity theft or the potential for identity theft that come to the person’s attention. Just having a program is not enough. The program must be flexible, adaptive and effectively enforced.

In recognition of the burden that compliance with the Red Flags Rule may impose on certain entities, 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, which is available at <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>.

---

*The FTC extended the enforcement date of the Red Flags Rule as it applies to non-financial institutions from November 1, 2009 to June 1, 2010.*

---

## Amendments to Massachusetts Security Regulation

The March 1, 2010 compliance date of the Massachusetts Regulation (201 CMR 17.00) remains unchanged though the Regulation has been finalized. As we have addressed in our previous Client Advisories, the breadth of the Regulation is impressive, extends to companies having information on Massachusetts residents whether or not the company is doing business in Massachusetts, and has already had impact nationally. There are no industry, private sector or out-of-state exemptions and no de-minimus number of employees under the regulations.

Under the Regulation, every person or company that owns or licenses personal information about a Massachusetts resident must develop, implement, maintain and monitor a comprehensive written information security program (“WISP”). The WISP must be reasonably consistent with industry standards and is required to contain administrative, technical and physical safeguards to ensure the security and confidentiality of such records. The provisions of the Regulation concerning WISPs are both broad and very granular at the same time and effectively demand an entire systems review as well as policy and other reconfigurations where necessary.

The final amendment filed on October 30, 2009 is the same as the amendment issued in August 2009 with two important clarifications. First, the latest amendment clarifies that businesses that have entered into contracts before March 1, 2010 have a two-year grace period to March 1, 2012 to amend or enter into contracts with third party service providers to require third party service providers to implement and maintain security measures for personal information in accordance with the Regulation. The two-year grace period applies only to contracts that have been entered into before March 1, 2010. For contracts entered into after March 1, 2010, there must be a provision requiring the third party vendor to have appropriate security measures for personal information. Given how often contracts renew automatically, it is advisable to add security provisions in now.

Second, the final Regulation now applies to persons that “store” personal information in addition to those that receive, maintain, possess or otherwise have access to personal information.

Although companies have about four months to comply, companies still have a lot of work to do before March 1, 2010, so that upon the effective date they are in compliance with this Regulation.

---

*The March 1, 2010 compliance date of the Massachusetts Regulation remains unchanged though the Regulation has been finalized.*

---

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 listed below:

Mark E. Schreiber, Partner

617.239.0585

[mshreiber@eapdlaw.com](mailto:mshreiber@eapdlaw.com)

Theodore P. Augustinos, Partner

973.520.2315

[taugustinos@eapdlaw.com](mailto:taugustinos@eapdlaw.com)

Barry J. Bendes, Partner

212.912.2911

[bbendes@eapdlaw.com](mailto:bbendes@eapdlaw.com)

Socheth Sor, Associate

860.541.7773

[ssor@eapdlaw.com](mailto:ssor@eapdlaw.com)

This advisory is published by Edwards Angell Palmer & Dodge for the benefit of clients, friends and fellow professionals on matters of interest. The information contained herein is not to be construed as legal advice or opinion. We provide such advice or opinion only after being engaged to do so with respect to particular facts and circumstances. The Firm is not authorized under the U.K. Financial Services and Markets Act 2000 to offer UK investment services to clients. In certain circumstances, as members of the U.K. Law Society, we are able to provide these investment services if they are an incidental part of the professional services we have been engaged to provide.

Please note that your contact details, which may have been used to provide this bulletin to you, will be used for communications with you only. If you would prefer to discontinue receiving information from the Firm, or wish that we not contact you for any purpose other than to receive future issues of this bulletin, please contact us at [contactus@eapdlaw.com](mailto:contactus@eapdlaw.com).

© 2009 Edwards Angell Palmer & Dodge LLP a Delaware limited liability partnership including professional corporations and Edwards Angell Palmer & Dodge UK LLP a limited liability partnership registered in England (registered number OC333092) and regulated by the Solicitors Regulation Authority.

Disclosure required under U.S. Circular 230: Edwards Angell Palmer & Dodge LLP informs you that any tax advice contained in this communication, including any attachments, was not intended or written to be used, and cannot be used, for the purpose of avoiding federal tax related penalties, or promoting, marketing or recommending to another party any transaction or matter addressed herein.

ATTORNEY ADVERTISING: This publication may be considered “advertising material” under the rules of professional conduct governing attorneys in some states. The hiring of an attorney is an important decision that should not be based solely on advertisements. Prior results do not guarantee similar outcomes.

**EDWARDS  
ANGELL  
PALMER &  
DODGE**

[eapdlaw.com](http://eapdlaw.com)