MINTZ

It's almost 2011. Do you know where your Red Flags Rule compliance program is?

December 07, 2010 | Blog | By Cynthia J. Larose

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

(UPDATED)

Late Tuesday, the House of Representatives passed the Red Flag Program Clarification Act of 2010 on a voice vote, clearing the way for President Obama's signature. The Clarification Act exempts doctors, lawyers, accountants and certain other professionals from compliance with the Red Flags Rule. As you may recall, we discussed lawsuits filed by the American Bar Association, the American Medical Association and the AICPA to exempt professionals from the definition of "creditors."

In all the flurry of privacy-related issues over the last few weeks, a deadline has been slowly creeping up.....remember the Red Flags Rule? (blog posts: June 29, 2010, May 24, 2010, December 3, 2009)

The December 31 deadline is looming for Federal Trade Commission (FTC) enforcement of the Red Flags Rule, which requires businesses and organizations to establish a program to detect and remediate identity theft -- and the program must have written policies and procedures and be approved by the Board of Directors.

The rule itself, which stems from the Fair and Accurate Credit Transactions Act, actually took effect on November 1, 2008. The FTC has delayed enforcement five times so companies could develop their compliance programs. According to the FTC, many didn't know they were engaged in activities that would cause them to fall under the rule, or hadn't even heard of it.

Despite the lead time, plenty of companies still aren't prepared for enforcement and even those who have actually implemented a program could be vulnerable. The Red Flags Rule requirements are very specific and without proper attention, covered entities may not be in compliance.

To review the applicability of the Red Flags Rule and how it might affect you, refer back to our earlier posts and threads referenced at the beginning of today's post. Although the Red Flags Rule has been out there since November of 2008 (and financial institutions have had to comply since then) confusion is rampant over who is a "creditor," what qualifies as a "covered account," and why some accounts are "covered" and some are not.

The Federal Trade Commission has a good website outlining the basics of the Red Flags Rule, with resources and FAQs. Below are some of the questions:

> **1. Can a consumer sue us under the Red Flags Rule?**
>
> **No, there is no private right of action. Only certain federal and state government agencies can enforce the Rule, but consumers can file a complaint with the FTC about a company's Program. The FTC uses complaints filed at to target its law enforcement efforts.**

2. If my business is covered by the Red Flags Rule, what will we need to show the FTC to prove we're complying? Is there a specific audit document we have to file or have available if asked?

The FTC does not conduct routine compliance audits. But the FTC can conduct investigations to determine if a business within its jurisdiction has taken appropriate steps to develop and implement a written Program, as required by the Rule. The FTC may ask the target of the investigation to produce copies of its Program and other materials related to compliance. The FTC also may interview officers, employees, or others who are familiar with the company's practices. If the FTC has reason to believe the Rule has been violated, it can bring an enforcement action.

3. I'm a creditor with consumer or household accounts, but I think it's very unlikely that an identity thief will try to defraud me. Do I still have to prepare an Identity Theft Prevention Program?

The Red Flags Rule requires all creditors with covered accounts to prepare an Identity Theft Prevention Program. At the same time, the Commission staff recognizes that your risk of identity theft may be so low that, as a matter of prosecutorial discretion, Commission staff would be unlikely to recommend bringing a law enforcement action under the following circumstances:

o You know your clients individually. For example, some medical practices and law firms are familiar with everyone who walks into the office. In such circumstances, the likelihood that an identity thief can defraud a business by impersonating someone else is extremely low.

o You provide services to customers in or around their home, such as by operating a lawn care or a home cleaning business. For these types of businesses, the risk of identity theft is extremely low because identity thieves generally do not want people to know where they live.

o You are involved in a type of business where identity theft is rare. For example, if there are no reports in the news, trade press, or among people in your line of business about identity theft and your business itself has not experienced incidents of identity theft, it is unlikely that identity thieves are targeting your sector.

Of course, from time to time you need to consider whether your identity theft risk has changed, warranting a different approach with respect to the Rule.

4. What are the penalties for non-compliance?

The FTC can seek both monetary civil penalties and injunctive relief for violations of the Red Flags Rule. Where the complaint seeks civil penalties, the U.S. Department of Justice typically files the lawsuit in federal court, on behalf of the FTC. Currently, the law sets $3,500 as the maximum civil penalty per violation. Each instance in which the company has violated the Rule is a separate violation. Injunctive relief in cases like this often requires the parties being sued to comply with the law in the future, as well as provide reports, retain documents, and take other steps to ensure compliance with both the Rule and the court order. Failure to comply with the court order could subject the parties to further penalties and injunctive relief.

5. What if I have a question not answered in these FAQs?

Your question may be answered in our booklet, *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, **our short articles on Red Flags compliance, or our form with step-by-step instructions on designing a Program for businesses and organizations at low risk for identity theft, all available at http://www.ftc.gov/redflagsrule.**

Are **you** ready? Happy New Year.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.