VENABLE® LLP

Articles

December 2010

Congress Clarifies and Limits FTC ID Theft Red Flags Rule to Take Effect January 1, 2011

AUTHORS

Thomas A. Cohn

Jonathan L. Pompan

RELATED PRACTICES

Antitrust

RELATED INDUSTRIES

Credit Counseling and Debt Services

Nonprofit Organizations and Associations

Education

ARCHIVES

2010 2006 2002
2009 2005 2001
2008 2004 2000
2007 2003

After a delay of more than two years, the Federal Trade Commission (the "FTC") will begin to enforce the Identity Theft Red Flags Rule ("Red Flags Rule" or the "Rule") that requires many organizations to implement a program to detect, prevent, and mitigate instances of identity theft.

The FTC had intended for the Red Flags Rule to take effect on November 1, 2008, but it had postponed enforcement several times due to concerns about whether "creditors" with covered accounts had enough time to develop and implement written identity theft programs; court challenges to the FTC's interpretation of "creditors," and a Congressional request to defer enforcement until changes to the scope of the Rule could be approved.

Now, in the wake of changes to the scope of the Red Flags Rule, the FTC is set to enforce it effective January 1, 2011. The Rule is part of the Fair and Accurate Credit Transactions Act, in which Congress directed the FTC and the federal banking agencies to develop regulations requiring "financial institutions" and "creditors" to address the risk of identity theft. The Red Flags Rule requires all such entities that have "covered accounts" to develop and implement written identity theft prevention programs to help identify, detect, and respond to patterns, practices, or specific activities – known as "red flags" – that could indicate identity theft.

Despite a carve-out for many professionals who take a fee after providing a service, the Red Flags Rule will still require a number of "financial institutions" and "creditors" to develop written programs to identify the warning signs of identity theft, spot them when they occur, take appropriate steps to respond to those warnings ("red flags"), and administer a written Identity Theft Prevention Program ("ITPP").

What changes did Congress make to the scope of the Rule's coverage?

On December 18, 2010, President Obama signed the Red Flag Program Clarification Act of 2010 (the "Act"). Effective immediately, the Act changes the definition of the word "creditor" under the Red Flags Rule to exclude most professionals who take payment after rendering services. Specifically, the measure excludes any entity that "advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person." In addition, the changes limit the definition of "creditor" under the Fair Credit Reporting Act to entities that use consumer reports, furnish information to consumer credit reporting agencies, or advance funds to or on behalf of a person.

Previously, the FTC said that under the Rule, the term "creditor" covered any providers of goods and services, including attorneys and health care practitioners who regularly grant their customers the right to defer payments. Now according to Senator Christopher Dodd (D-CT), "lawyers, doctors, dentists, orthodontists, pharmacists, veterinarians, accountants, nurse practitioners, social workers, other types of health care providers and other service providers will no longer be classified as 'creditors' for the purposes of the red flags rule because they do not receive payment in full from their clients at the time they provide their services, when they do not offer or maintain accounts that pose a reasonably foreseeable risk of identity theft."

The Red Flags Rule defines "financial institutions" as institutions under the jurisdiction of the federal banking regulatory agencies and/or the National Credit Union Administration, and any other person, that directly or indirectly, holds a transaction account belonging to a consumer.

What is a "covered account"?

Only "financial institutions" and "creditors" that have "covered accounts" need to have a written ITPP. "Covered accounts" are those used mostly for personal or family or household purposes. According to the FTC, "covered accounts" include credit card accounts, mortgage loans, automobile loans, margin

accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. In addition, an account can still be "covered" if there is a reasonably foreseeable risk of identity theft to the account holder, based on activity during the opening, accessing, or transactional use associated with that account.

What does the Red Flags Rule require?

Under the Red Flags Rule, "financial institutions" and "creditors" that have "covered accounts" must develop a written ITPP that identifies and detects the relevant warning signs – or "red flags" – of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The ITPP must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the ITPP. The ITPP must be managed by the Board of Directors or senior employees of the "financial institution" or "creditor," require oversight of any service providers, and include appropriate staff training.

Even a low-risk covered entity needs to have a written ITPP that is approved either by its Board of Directors or an appropriate senior employee. Since risks change, there is an obligation to assess the program periodically to keep it current. Likewise, because business models and services change, organizations should periodically assess whether or not they are a covered entity subject to the Red Flags Rule and whether they are in compliance with the terms of the Rule.

What elements must an ITPP include?

The ITPP must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable a "financial institution" or "creditor" to:

. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the ITPP;
. Detect red flags that have been incorporated into the ITPP;
. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
. Ensure that the ITPP is updated periodically to reflect changes in risks of identity theft.

The FTC also issued guidelines to assist financial institutions and creditors in developing and implementing an ITPP, including a supplement that provides examples of red flags.

Do nonprofit organizations have to comply with the Red Flags Rule?

There is no exception from the Red Flags Rule for nonprofit organizations. Nonprofit entities that fall under the definition of either a "financial institution" or "creditor" that have "covered accounts" are required to implement an ITPP.

What is the potential liability for noncompliance with the Red Flags Rule?

The FTC can obtain civil penalties of up to $3,500 for each violation of the Rule by entities within its jurisdiction. If a person, including a company, is found to be a "financial institution" or "creditor" but does not have the required ITPP, the number of violations could equal the number of covered accounts that should have been protected by the required program. There also could be state agency enforcement, with up to $1,000 for each willful violation, plus costs and reasonable attorneys' fees if that enforcement is successful. While private causes of actions cannot be brought for Rule violations, identity theft victims could bring claims under other theories of liability.

By when must covered entities comply with the Rule?

Many organizations will be considered "financial institutions" or "creditors" under the Red Flags Rule, and many of these organizations will have "covered accounts" as defined by the Rule. Given that the FTC is set to enforce the Rule effective January 1, 2011, it is crucial that all organizations coming within the Rule's coverage have an ITPP in place by December 31, 2010. Given the risk-based nature of the Red Flags Rule's regulations, the requirements are flexible and may be tailored to the degree of identity theft risk faced by the particular company and activity.

For additional information:

For a full summary of the Red Flags Rule, see the following articles by Venable attorneys:

- "**FTC Issues Business Guidance for Identity Theft Red Flags Rule Compliance**"
- "**Assessing Associations' Identity Theft Red Flags and Risks**"
- "**The 'Red Flags' Rule: What Independent Schools Must Know About Complying With New**

Requirements for Fighting Identity Theft"

* * * * * * *

*For more information, please contact Thomas A. Cohn at 212.370.6256 or **tacohn@Venable.com**, or Jonathan L. Pompan at 202.344.4383 or **jlpompan@Venable.com**.*

This article is not intended to provide legal advice or opinion and should not be relied on as such. Legal advice can only be provided in response to a specific fact situation.