

The FACTA Red Flags Rule: A Primer

Contributed by Tanya L. Forsheit, InfoLawGroup LLP

On November 9, 2007, the Federal Deposit Insurance Corporation, Federal Reserve Board (FRB), Office of the Comptroller of the Currency, and the Office of Thrift Supervision (collectively, banking agencies), along with the National Credit Union Administration (NCUA) and the Federal Trade Commission (FTC), issued a joint final rule (the Red Flags Rule) pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA).¹ The Red Flags Rule requires covered entities to design and implement written programs and policies to detect, prevent and mitigate identity theft connected with the opening of a "covered account" or any existing covered account.²

Overview of the Red Flags Rule

The Red Flags Rule applies to certain "covered entities", as defined below. At a high level, the Red Flags Rule requires the following of covered entities: (1) establish a written Identity Theft Prevention Program, including the following elements: (a) identification of red flags, (b) detection of red flags, (c) appropriate response to detected red flags, and (d) updates; and (2) administer the program by, among other things: (a) obtaining the approval of the board of directors, (b) designating personnel to oversee and administer the program, (c) training staff, and (d) exercising oversight of service provider arrangements.

Red flags include, but are not limited to, the following:

- A fraud alert, credit freeze, or address discrepancy that is included with a consumer report or provided by a credit reporting agency;
- A consumer report that indicates a pattern of activity which is inconsistent with the history and usual pattern of activity of an applicant or customer;
- Documents, applications, or photo identification that appear to have been altered or forged, or give the appearance of having been destroyed and reassembled;
- Other information on the identification that is not consistent with readily accessible information on file with the financial institution or creditor, such as a signature card or a recent check;
- Receiving personal identifying information that is inconsistent when compared to other such information on file with the financial institution or creditor or provided by the customer, or otherwise inconsistent when compared against external information sources used by the financial institution or creditor;
- Receiving personal identifying information that is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor;
- The Social Security number, address or telephone number that is provided is the same as that submitted by other customers or by an unusually large number of other persons opening accounts;

- Shortly following the notice of a change of address for a covered account (as defined below), the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account; and/or
- A covered account is used in a manner that is not consistent with established patterns of activity on the account.³

More examples of potential red flags can be found in 12 C.F.R. Supplement A to Appendix J to Part 222.⁴

Who Must Comply with the Red Flags Rule?

The Red Flags Rule applies to all financial institutions and creditors that hold or maintain "covered accounts," which include: (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, and (2) any other account for which there is a reasonably foreseeable risk of identity theft to customers or to the safety and soundness of the financial institution or creditor.⁵ "Covered accounts" include accounts located in the U.S., including accounts established in the U.S. by non-U.S. residents.⁶ All banks, savings associations, and credit unions are covered by the Red Flags Rule as "financial institutions," whether or not they hold a transaction account belonging to a consumer.⁷

Financial institutions for purposes of the Red Flags Rule include banks, mortgage lenders, savings and loan associations, mutual savings banks, credit unions, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer. Creditors include persons or businesses that regularly arrange for the extension, renewal, or continuation of credit, as well as assignees of an original creditor who participates in the decision to extend, renew or continue credit.

The Red Flags Rule does not apply to the foreign branches of U.S. banks, but, as a matter of safety and soundness, the agencies strongly encourage financial institutions to implement an effective Identity Theft Prevention Program throughout their operations, including in their foreign offices, consistent with local laws.⁸ A broker, dealer, investment advisor, or investment or insurance company that is a "financial institution" or "creditor" under the Fair Credit Reporting Act (FCRA) is covered by the Red Flags Rule, including any such entity that is a subsidiary of a bank or savings association.⁹ Corporate credit unions are also covered by the Red Flags Rule.¹⁰ Furthermore, if a consumer loan is purchased by another financial institution or creditor, then that entity becomes responsible for applying its Identity Theft Prevention Program to the loan as an existing covered account.¹¹

Since 2007, the FTC has issued several clarifying statements regarding the types of businesses covered by the Red Flags Rule. It has taken the position that the Red Flags Rule applies to any company that "regularly defers payment for goods or services."¹² This can include any company that does not require payment at the time goods or services are provided. For example, health care providers who regularly defer payment for medical services must comply with the Red Flags Rule, according to the FTC, and in a March 2009 entry in its *How-To Guide for Business*¹³, the FTC

noted that the Red Flags Rule also applies to retailers that offer financing or help consumers get financing from others.

The FTC's statements, and the accompanying controversy regarding the scope of coverage of the Red Flags Rule, revolve around the term "creditor," defined in the Red Flags Rule by reference to the Equal Creditor Opportunity Act (ECOA). Under the ECOA, "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." The ECOA defines "credit" as "the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor."¹⁴

In a letter to the American Medical Association, the FTC cited the FRB's elaboration on the definition of creditor and credit. Specifically, the FTC noted that "In its Official Staff Commentary to Regulation B, the Federal Reserve Board makes clear that the terms 'creditor' and 'credit' under the ECOA should be interpreted broadly so as to include all entities that defer payments, even in the normal course of a traditional billing process."¹⁵

The FTC's interpretation of "creditor" potentially extends the Red Flags Rule to an extraordinarily large portion of the economy, including virtually any company that does not require immediate payment for goods or services. This could include hospitals, insurance companies, telecommunication companies, doctors and a host of other businesses that provide products or services and bill for them later. While the number of entities that need to comply with the Red Flags Rule may be significant, the FTC also recognizes that entities posing a lower risk of identity theft may comply with the Red Flags Rule by implementing relatively simple written Identity Theft Prevention Programs. The difference between low-risk and high-risk will vary depending on the particular circumstances.

Most recently, the controversy grew when United States District Judge Reggie B. Walton of the United States District Court for the District of Columbia ruled in *American Bar Association v. Federal Trade Commission*¹⁶ that the FTC exceeded its authority by applying the Red Flags Rule to practicing lawyers.¹⁷ In addition, not long after the court issued this ruling from the bench, the American Institute of Certified Public Accountants ("AICPA") filed a similar lawsuit against the FTC seeking an injunction barring application of the Red Flags Rule to its members.¹⁸

Is the Red Flags Rule Being Enforced?

The Red Flags Rule took effect on January 1, 2008. The compliance deadline for financial institutions regulated by the banking agencies, the NCUA and the Securities and Exchange Commission was November 1, 2008. The FTC has extended the deadline for enforcement several times, specifically from November 1, 2008, to May 1, 2009, to August 1, 2009, to November 1, 2009, and finally to June 1, 2010.¹⁹ The FTC's continuances of the enforcement deadline do *not* extend to financial institutions and creditors subject to the jurisdiction of the banking regulators and the NCUA.

Conclusion

It remains to be seen whether the FTC follows through with its current plan to begin enforcing the Red Flags Rule with respect to organizations subject to its jurisdiction on June 1, 2010. In the meantime, the Red Flags Rule remains in effect as to all financial institutions and creditors, and those organizations must move forward with development and implementation of their written Identity Theft Prevention Programs.

Tanya Forsheit is a Founding Partner of InfoLawGroup LLP, www.infolawgroup.com. She is based in Los Angeles. Ms. Forsheit spent 12 years as a litigator and privacy/data security counselor at Proskauer Rose, where, most recently, she was Co-Chair of the Privacy and Data Security group. In 2009, Ms. Forsheit was named one of the Los Angeles Daily Journal's Top 100 women litigators in California. Certified as an information privacy professional by the IAPP, Ms. Forsheit works with clients to address legal requirements and best practices for protection of customer and employee information. She can be reached at tforsheit@infolawgroup.com.

¹ 15 U.S.C. § 1681m(e).

² 72 Fed. Reg. 63,718.

³ See, e.g., 12 C.F.R. Supplement A to Appendix J to Part 222.

⁴ *Id.*

⁵ See, e.g., 12 C.F.R. § 222.90(b)(3).

⁶ *Frequently Asked Questions (FAQs)* issued June 11, 2009, <http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf>.

⁷ *Id.*

⁸ *Frequently Asked Questions (FAQs)* issued June 11, 2009, <http://www.ftc.gov/os/2009/06/090611redflagsfaq.pdf>.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² See, e.g., Steven Toporoff, attorney with the FTC's Division of Privacy & Identity Protection, *The Red Flags Rule: Compliance Tips for Companies Offering Services In and Around the Home* (May 2009), available at <http://www.ftc.gov/bcp/edu/pubs/articles/art15.shtm>.

¹³ *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, available at <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>.

¹⁴ 15 U.S.C. § 1691a(d).

¹⁵ Letter from Eileen Harrington, Acting Director of Bureau of Consumer Protection, FTC, to Margaret Garikes, Director of Federal Affairs, American Medical Association, dated February 4, 2009, at 5 & n. 21 (citing "Official Staff Commentary, 12 CFR 202.1(a)-1 (recognizing that the term 'credit' under the ECOA is intentionally broader than the definition of 'credit' under the Truth in Lending Act and applies to any 'deferral of the payment of a debt')").

¹⁶ 2009 BL 257706, Civil Action No. 09-1636 (RBW) (D.D.C. Dec. 1, 2009).

¹⁷ *Id.* at 18.

¹⁸ See AICPA Complaint, available at <http://www.aicpa.org/download/news/2009/AICPA-Complaint.pdf>.

¹⁹ See FTC Press Release, available at <http://www.ftc.gov/opa/2009/10/redflags.shtm>.