

“Red Flags Rule” – Will You Be Compliant or Complacent?

By Alan S. Wernick

The federal “Red Flags Rule” is designed to minimize identity theft. The failure of covered entities to comply can have several consequences, including civil penalties, injunctions, annual reporting, government oversight of the non-compliant business, and loss of trust by the customers of the business.

An amendment to the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”) requires covered entities to create programs which must provide for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft. The Federal Trade Commission (“FTC”), the federal bank regulatory agencies (including the Office of the Comptroller of the Currency, the Federal Reserve, the Federal Deposit Insurance Program, and the Office of Thrift Supervision), and the National Credit Union Administration have issued regulations concerning this Red Flags Rule (the “Rule”).

In October 2008 the FTC granted a six-month delay of enforcement of the Rule requiring covered entities under its jurisdiction to have identity theft prevention programs in place. This enforcement delay was limited to the Identity Theft Red Flags Rule, and did not extend (a) to the rule regarding address discrepancies applicable to users of consumer reports, or (b) to the rule regarding changes of address applicable to card issuers. The FTC delay did not affect other federal agencies’ original November 1, 2008, enforcement date of the Rule.

May 1, 2009, marks the beginning of the FTC enforcement of the Rule. The FTC’s announced purpose for their delay in enforcement is to allow covered entities sufficient time to

establish and implement appropriate identity theft prevention programs in compliance with the Rule. Will you be ready?

What Are The Red Flags Rule And How Will You Comply With Them?

How you comply with the Rule depends on your business, the type of sensitive consumer data your business collects which is subject to the Rule, and how your business handles that data. Essentially the Rule requires you to develop a written program that identifies and detects relevant identity theft warning signs – i.e., “red flags.” Your written program must also describe your responses that would prevent and mitigate identity theft as well as set forth detailed information as to how you will update the written program. The Rule states that the written program must initially be managed by the Board of Directors or, if the business does not have a Board of Directors, by senior employees. The business must have an annual review of the program, provide appropriate staff training, and provide for oversight of any third-party service providers.

The Rule set forth numerous examples of types of red flags, which fall into five categories:

- Alerts, notifications, or warnings from a consumer reporting agency;
- Suspicious documents;
- Suspicious personally identifying information, such as a suspicious address or SSN that is listed on the Social Security Administration’s Death Master File;
- Unusual use of, or suspicious activity relating to, a covered account;

- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts held by the financial institution or creditor.

In 2005 ChoicePoint, Inc., suffered a major data breach involving some 163,000 records. ChoicePoint ultimately settled with the Federal Trade Commission for \$10 million in civil penalties and \$5 million for consumer redress. This \$15 million was in addition to the other costs (e.g., attorney fees, security consultant fees, customer notifications, etc.) incurred as a result of the breach. In the ChoicePoint situation the identity thieves set up bogus ChoicePoint accounts which they used to obtain the personal identifiable information records. If the Rule had been effective in 2005 and ChoicePoint in compliance, perhaps the data breach could have been avoided, or at least minimized both in terms of the number of records breached and the total cost to ChoicePoint resulting from the breach.

Who Must Comply With The Red Flags Rule?

The Rule applies to “financial institutions” and “creditors” with “covered accounts.” Where the enforcement net widens is in the definition of “creditors” with “covered accounts.” This is because the Rule defines a “creditor” as any entity that regularly extends, renews, or continues credit; that arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Specifically identified as “creditors” are finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies; plus non-profit and

government entities that defer payment for goods or services. Other “creditors” deferring payments on a regular basis may include retailers and hospitals.

The expanded coverage of the Rule arises in part through the definition of a “covered account.” This definition is integral to the underlying policies of the Red Flags Rule – the prevention of identity theft. A “covered account” is defined as an account used mostly for personal, family, or household purposes, and involves multiple payments or transactions. This includes financial accounts such as credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts, plus any account “that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.” This definition would include any account that may be vulnerable to identity theft such as a small business or sole proprietorship account. Thus, if your business is a steward of data that, if breached, presents a reasonably foreseeable risk of identity theft, then the Rule may apply.

One may argue that any new rule or regulation is overly burdensome. Nevertheless, for those businesses now leading or on track to become the leaders in their respective industries the Red Flags Rule may provide one benchmark for best practices in protecting the personal identifiable information of the customers and employees of the business. The health care services industry is already subject to a number of privacy related regulations. Two examples being the Health Insurance Portability and Accountability Act (“HIPAA”), and the American Recovery and Reinvestment Act of 2009 (“ARRA”), Title XIII – the Health Information

Technology for Economic and Clinical Health Act (the “HITECH Act”) – which indicates a new phase in the evolution of federal law governing the privacy and security of medical information. Likewise, the financial services is subject to a number of privacy related regulations, such as the Gramm-Leach-Bliley Act (“GLB”).

With medical identity theft on the rise, much of the enforcement activity in medical identity theft cases has come from the offices of the Attorney General in various states rather than through HIPAA enforcement. Since the requirements of the state data breach laws vary, the Red Flags Rule may prove less of a burden to the health care industry than might appear from a first look at the Rule, and proper and consistent compliance with the Rule may minimize the exposures that trigger the data breach laws in the first place.

What Might Happen If You Fail To Comply With The Red Flags Rule?

Typical FTC enforcement activities of the Red Flags Rule may include requesting injunctive relief, monetary damages, and increased government oversight of your business (including annual reporting of your compliance for possibly twenty years). This is in addition to the value of management’s time that will have to be focused in a crisis mode upon receipt of notice of an enforcement action, court costs, consultant fees, and attorney fees to respond to the enforcement action. But all of these costs may pale in comparison to the cost to your business resulting from a loss of trust by your customers due to a data breach, particularly when the customers are victims of identity theft traced back to your business. Which costs less: prevention or clean-up? Taking the time now to understand the data your business uses, how the Red Flags Rule apply to your business, and engaging in preventive planning to comply with

the Red Flags Rule should cost your business less. As Ben Franklin said: “An ounce of prevention is worth a pound of cure.” Ignoring the Red Flags Rule could cause your business’s bottom line to see red.

© 2009 Alan S. Wernick. WWW.WERNICK.COM All rights reserved.

About The Author: Since 1982 [Alan S. Wernick](http://WWW.WERNICK.COM) has been practicing computer law / cyberspace law / information technology law, data privacy, and intellectual property law. He has a background in computer programming and accounting. Alan is admitted to practice in IL, NY, OH, and DC. Additional information is available at WWW.WERNICK.COM. He can be reached via e-mail at ALAN@WERNICK.COM.