

Account: 23556-234-00 086-02

NTS by type of

Savings Grants (CESGs)  
amount in the month

BO  
LLIV

LLOS

BNS0111300

ment p  
units listed in th  
ay have

curities Inc.

# Red Flags Rule: Will you be compliant or complacent?

---

Under the federal Red Flags Rule, businesses are now obligated to actively recognize, detect and respond to telltale signs of identity theft.

---

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 noncompliant business and loss of trust by customers of the business. An amendment to the Fair and Accurate Credit Transactions Act of 2003 (FACTA) requires covered entities to create programs that 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 Insur-

ance Program and the Office of Thrift Supervision), and the National Credit Union Administration have issued regulations concerning this Red Flags Rule.

Since the original date of Nov. 1, 2008, the FTC has twice extended its enforcement of the rule requiring covered entities under its jurisdiction to have identity theft prevention programs in place. In October 2008, the FTC issued its first delay for six months. Then on April 30, 2009, the FTC again delayed its enforcement until Aug. 1, 2009. Both FTC enforcement delays were limited to the Red Flags Rule, and did not extend to the FACTA amendments regarding addressing discrepancies applicable to users of consumer reports, or changes of address applicable to card issuers. The FTC delay

*by Alan S. Wernick*

did not affect other federal agencies’ original Nov. 1, 2008, enforcement date.

August 1, 2009, now marks the beginning of the FTC enforcement of the rule. The FTC’s announced purpose for its 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 is the Red Flags Rule and how will you comply with it?**

How you comply with the rule depends on your business, the type of sensitive consumer data your business collects that 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, 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 sets 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 personal identifying information, such as a suspicious address or Social Security number that is listed on the Social Security Administration's death master file;
- Unusual use of, or suspicious activity relating to, a covered account; and
- 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 FTC 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 in effect in 2005 and had ChoicePoint been 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 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 ex-

tends, 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 and telecommunications companies, and nonprofit 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 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 of this are the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), part of the American Recovery and Reinvestment Act of 2009. HITECH indicates a new phase in the

evolution of federal law governing the privacy and security of medical information. Likewise, financial services are subject to a number of privacy-related regulations, such as the Gramm-Leach-Bliley Act.

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.

### **What 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 20 years). This is in addition to the value of management's time that will have to be focused in a crisis mode on 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 applies 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' bottom line to see red. ■

## **Author bio**



Alan S. Wernick is with FSB Legal Counsel. He focuses his practice on information technology law, intellectual property law and privacy law. He is a member of the bar in Ohio, Ill., N.Y. and the District of Columbia. © 2008 - 2009 ALAN S. WERNICK.

T: 847.786.1005

M: 847.770.1355

E: WERNICK@FSBLEGAL.COM

Web: WWW.FSBLEGAL.COM

Listing of articles & lectures are available at WWW.WERNICK.COM.