INSIGHT

Red Flags Rule Enforcement by FTC Begins August 1, 2009

June 2009

Introduction

The Red Flags Rule is designed to protect personal identifiable information from data thieves. While many people believe that data protection regulation applies only to hospitals and banks, data thieves are attacking other businesses, so regulation has expanded.

The Red Flags Rule applies to any business or individual that provides a product or service for which payment is made after the product or service is delivered. The deadline for compliance is August 1, 2009, after which date the Federal Trade Commission (FTC) will begin enforcement of the Rule.

Why are businesses other than hospitals and banks targeted?

Banks and hospitals must comply with the Red Flags Rule, but other businesses also need to protect sensitive data. As hospitals and banks have enhanced their protection of data, cybercriminals increasingly are attacking easier targets. To respond to this problem and protect people from data theft, law enforcement has begun focusing on data kept by Main Street businesses.

What happens if a business does not comply?

The goal of reducing identity theft is a worthy cause, but adhering to more regulations in the current tough market conditions may be difficult. However, attempting to avoid the expense of compliance may not be in the best interest of a business. For a business that finds itself the victim of a data security breach in which personal identifiable information could have been accessed, failure to comply with the Red Flags Rule may prove significantly damaging.

Press reports about data breaches cause serious damage to the hard-earned reputation of a business. The personal data aggregation company, ChoicePoint, came under heavy criticism when cyber criminals stole the personal identifiable information of at least 163,000 Americans in 2005. TJX, the discount retailer, gained international disrepute when it was discovered that 45.6 million credit and debit card numbers stored on their databases had been stolen.

When customers are exposed to data theft because a business did not take simple precautions required by federal regulations, local newspapers and radio coverage of the
breach can be harsh. Word of mouth can be even worse. Arguing unawareness of the Red Flags Rule most likely would be used as further proof that the business was clueless and careless.

Data breaches routinely result in lawsuits and compliance with the Red Flags Rule is strong evidence that a business was not negligent. Failure to comply, on the other hand, may be used as evidence that the business failed to meet established federal regulations for safekeeping personal identifiable data. Litigation outcomes may be strongly impacted by whether a business is, or is not in compliance with the Red Flags Rule.

In addition to private lawsuits that may result from a data breach, federal government regulators including the FTC are authorized to enforce compliance with the Red Flags Rule. Monetary penalties of up to $3,500 per violation may be assessed. Violation of the Red Flags Rule also could result in prosecution for violation of state consumer protection or deceptive trade practices laws. These state laws often include language permitting private individuals to sue and recover treble damages, attorneys’ fees and/or litigation costs.

**What is required?**

The Rule requires senior management to adopt and implement a written Red Flags Rule compliance plan. The plan must identify indicators of potential data breaches that could occur in the normal course of operations. In addition to identifying potential data breach indicators – so-called "red flags" - the written plan needs to specify procedures that are to be implemented when a red flag indicates a potential data breach. In addition to procedures for identifying and handling red flag situations, the written plan also needs to specify when and how red flag identification and procedures will be regularly updated.

Compliance with the Red Flags Rule can be fairly simple. Often, a few individuals have enough information about the ways in which the business obtains and keeps personally identifiable information to identify how an attempt at data theft might happen, and what would indicate that a data theft happened. For example, laptop computer theft is one of the most frequent causes of data security breaches. If a business uses laptop computers, and a laptop is stolen, the theft would be a red flag that identity theft might follow. If a laptop is stolen, the company's procedure would be to block the laptop from accessing the company network, and to determine what information was on the laptop when it was stolen. If personal identifiable information was on the laptop when it was stolen, the company would comply with applicable privacy laws, appropriately notifying law enforcement and potentially impacted people of the laptop theft.

The company also may take other steps, such as working with potentially impacted people and the credit bureaus to protect individuals from damage caused by identity theft. In addition, the company could adopt a procedure to annually review its laptop theft Red Flag Rules and train staff members on laptop theft red flag procedures. Senior management needs to approve the written plan for laptop computer theft and oversee implementation to comply with the Red Flags Rule.

For each red flag a company identifies, a written procedure must be developed and approved for addressing the red flag, including regular training of staff and periodic updates of the red flags and procedures.

We have the experience to help you make compliance with the Red Flags Rule simple.

For more information, please contact Adam R. Bialek via e-mail at adam.bialek@wilsonelser.com or 914.323.7000.