1115 BROADWAY 12TH FLOOR, NEW YORK, NY 10010
212-710-2643 | linfo@WRLAWFIRM.com | www.WRLAWFIRM.com

THE FIVE MINUTE GUIDE TO THE FTC'S RED FLAG DATA BREACH RULES

Small business must contend with an ever increasing array of digital and electronic issues that can lead to disastrous consequences if not proactively addressed. Key among those is a proactive approach to the breach of consumer data.

The world of identity theft and its legal consequences are not limited to big credit companies. Main street businesses, with online portals, or credit/payment card facilities of some kind are just as much at risk. And if the rhetoric doesn't scare, then the numbers should as the Identity Theft Resource Center states the business sector increased to 41% of all the publicly reported breaches in 2009. As a result, all small businesses need to face the real danger of data breaches, which are not limited to malicious third parties, but can also arise from employee error. And these businesses should understand that risk control policies must be undertaken to prevent data breaches and robustly address them should they occur.

Secondly, the problem isn't simply a business issue anymore; it's very much a legal issue with real consequences. Various states and the federal government are formalizing statutory penalty schemes for business that do not proactively address data breaches. That alone should be cause to examine one's own data breach policy.

I. In fact, the Federal Trade Commission (FTC) has already acted.

Under the FTC's "Red Flags Rule," financial institutions and creditors are required to implement a written identity theft prevention program that, among other things, is set to detect warning signs ("red flags") of identity theft risks, take concrete steps towards prevention, and limit damages if theft occurs. Critically, the term "creditor" is broadly defined to include nearly all companies that provide goods or services via credit/payment card customer payment. And these businesses face stiff financial penalties for Red Flags violations.

A. The following measures should be undertaken now to avoid running afoul of the new FTC "Red Flag" regulations:

1. **Employee Training**

First and foremost, businesses need to recognize the role of employee errors in creating data breaches. Hence, training employees to identify and address potential breaches is key. Training should guide them to report an identified breach or risk of breach to a specific superior for quick action. Some also advocate creating anonymous reporting mechanisms to remove employee fear of reprisal.

2. **Implement a Data Breach Notification Policy**

Businesses should craft and make available a written policy that lays out to customers how the business will notify customers in the event of a data breach. Typically, an email is the most efficient and cost

effective method. Certain states have specific requirements on notification delivery; hence consulting that state's statute might be in order.

3. **Aggressive Fact Inquiries**

Businesses faced with data breaches should not turn the other cheek. Rather, aggressively probing and taking stock of the breach is the best practice to determine: the scope and nature of the compromised information; the time and manner in which the breach occurred; the source of the breach, external, or internal, etc. These determinations can mitigate future risk and provide invaluable assistance in dealing with any current breach.

4. **Leverage Counsel**

Leveraging outside counsel and risk experts, the instant a breach or a significant risk of breach occurs, is both a necessary damage control step and PR maneuver. By not only guiding the business through any legal or regulatory mazes (such as specific notice requirements to the public and/or government) that may confront it during a data breach crisis, retained counsel signals to the public that the business is taking the breach seriously and is prepared to engage experts in order to best solve the problem.

5. **Notify Financial Institutions**

In the event financial information (e.g., credit/payment card numbers, etc.) has been breached, businesses should waste no time in contacting any bank or merchant company that oversees credit/payment card processing.

6. **Notify Affected Customers per Policy**

Once a breach has occurred a business should execute the notification procedures laid out in its own policy. Per such notification, the business should provide a clear and honest explanation of the nature of the breach as well as the actual steps the business is taking to address the issue.

II. New York's Information Security Breach and Notification Act gives a Window into State Legislation Counterparts

In addition to the FTC rules, if a data breach of "private information" occurs with a business operating in New York, the sate level act requires notification to NY state residents. Moreover, if a third party is not the owner of the data but processes such data and a breach occurs, they must notify the owner, who in turn inherits the notification obligation. Penalties for non-compliance can range from $5,000 to $150,000.

III. Additional information on the FTC's Red Flags Rule can be found here.