LEGAL UPDATES

PUBLISHED: MAY 19, 2010

“Red Flag” Warning For Businesses To Fight Identity Theft: June 1 Deadline for Compliance with Federal Regulations

Service

Data Privacy & Cybersecurity

The Federal Trade Commission (FTC) and other federal agencies issued a “Red Flag” that requires most businesses to proactively combat the risk of identity theft and protect the personal information of customers and clients. The federal regulations require businesses to implement a full, written Identity Theft Prevention Program with Board-level approval and oversight by June 1, 2010.

The Red Flags Rules are a product of the Fair and Accurate Credit Transaction Act (FACT Act) and the rule-making authority of several federal agencies. Businesses that do not comply with the FACT Act provisions risk substantial statutory fines and intrusive regulatory investigations.

June 1 will be here quickly. It is not too late to begin or finalize compliance with the Red Flag Rules and other information security requirements.

Who Must Comply?

The Red Flag Rules apply to financial institutions and creditors that use personal information from their customers and maintain “covered” accounts for those customers. Examples of businesses subject to the Red Flag Rules include:

Any business that arranges or extends "credit":

Cable/internet service providers

Car/boat dealers

Credit card issuers/providers

Mortgage lenders

Retailers

Telecoms

Third-party vendors

Utilities

Any business that allows for deferred or delayed payments to sell goods or services:

Accounting firms

Building and design services

Law firms

Professional consulting practices

Schools, colleges and universities

Financial institutions:

Banks

Commercial lenders

Financial advisors and service providers

Mortgage brokers

Securities brokers/dealers

Subsidiaries of foreign banks

What This Means To You

Compliance with the federal mandate by the June 1, 2010, deadline will require substantial planning and immediate action. While there are many short-cut opportunities, an appropriate written Identity Theft Prevention Program may require a series of investigations and risk assessments. Each company faces a unique set of identity theft risks; each compliance program should be designed specifically to address those unique risks.

The first step in your plan for compliance should be to determine whether the Red Flag Rules apply to your business. Next, you need to evaluate the unique risks of unauthorized access to personal information in your organization. From there, the Red Flag Rules require that you create and

implement a full, written program that is appropriate for the size and scope of your business in light of the risks to the personal information that you retain. Last, your Red Flags program should coordinate and harmonize with your organization's other Information Security policies and procedures, your Human Resources and training programs, and your IT practices.

Contact Information
Please contact your Husch Blackwell attorney or an attorney from our Privacy & Data Security practice for more information on FACT Act Red Flags and assistance in creating a comprehensive FACT Act Identity Theft compliance solution.

Husch Blackwell Sanders LLP regularly publishes updates on industry trends and new developments in the law for our clients and friends. Please contact us if you would like to receive updates and newsletters, or request a printed copy.