Privacy and Security Alert: Last Call for "Red Flag" Compliance Planning

7/23/2009

As we reported in our May 1, 2009 Client Alert, the Federal Trade Commission (FTC) issued a last-minute reprieve to businesses struggling with development of Red Flag identity theft prevention programs. Creditors and financial institutions were given more time to develop and implement written identity theft prevention programs, but the reprieve is coming to an end. The FTC is scheduled to **begin enforcement of the new "Red Flags Rule" on August 1, 2009**.

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) directed financial regulatory agencies—including the FTC—to set forth rules requiring "creditors" and "financial institutions" with covered accounts to implement programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

The definition of "creditor" in the Red Flag Rules is very broad—and includes far more than the traditional notion of a business that extends credit. "Creditors" are any entities that regularly extend or renew credit—or arrange for others to do so—*and regularly permit deferred payments for goods or services.* Some examples are:

- Businesses that provide services and bill later, including many providers of professional services
- Non-profit and government entities that defer payment for goods or services
- Retailers that issue credit cards, or arrange for a third party to issue credit cards
- Finance companies
- Automobile dealers that provide or arrange financing
- Mortgage brokers
- Utility companies
- Telecommunications companies.

"Financial institutions" include entities that offer accounts that enable consumers to write checks or make payments to third parties through other means, such as telephone transfers.

By August 1, 2009, these "creditors" and "financial institutions" with covered accounts will need to implement a written identity theft prevention program containing policies that identify, detect, and respond to "red flags"—patterns, practices, activities, or incidents that potentially implicate identity theft—while also ensuring the program is reviewed and updated in order to adjust to changing and developing identity theft risks.

Besides containing the four fundamental elements—identify, detect, respond, and ensure—each written identity theft prevention program must outline the patterns, practices, activities, and/or incidents that constitute "red flags" of identity theft, which can include:

- Alerts, notifications, or warnings received from a consumer credit reporting agency

- The submission of suspicious documentation that appears to be altered or inconsistent with other documents on file
- The submission of suspicious Personally Identifying Information (PII), such as multiple addresses
- Unusual or suspicious use of, or access to, a covered account
- Notification from consumers or law enforcement authorities indicating suspected or actual identity theft.

Small businesses and those who are at low risk for identity theft must still have a "Red Flag program," but the FTC provides guidelines and a sample program for qualifying entities, including those that know their customers personally and are at a low risk for identity theft. Under the FTC's guidance, low-risk businesses include:

- Businesses, such as doctor or lawyer practices, that are personally familiar with their customers and therefore are unlikely to be fooled by impostors
- Businesses that provide services at customers' homes
- Businesses that have never received a complaint or discovered an incident of identity theft
- Industries in which identity theft is uncommon.

Those businesses that do not fall into the category of "low risk" are required to undertake a more in–depth review of the risks, and should be implementing a substantially more detailed identity theft prevention program by the August 1, 2009 deadline.

Mintz Levin's Privacy and Security group has been working with clients on the development of Red Flag compliance programs. We can help conduct risk assessments and develop or review your Red Flag program and policies, including employee training; advise on duties to detect, prevent, and mitigate identity theft; analyze and prepare vendor agreements that comply with your Red Flag duties; and advise senior management on responsibilities under the regulations.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

Cynthia Larose, CIPP
(617) 348-1732
CLarose@mintz.com

Michele Floyd
(650) 251-7723
MFloyd@mintz.com

Bruce D. Sokler
(202) 434-7303
BDSokler@mintz.com

Elissa Flynn-Poppey
(617) 348-1868
EFlynn-Poppey@mintz.com

Robert G. Kidwell
(202) 661-8752
RGKidwell@mintz.com

Julia M. Siripurapu
(617) 348-3039
JSiripurapu@mintz.com