DEAN MEAD

Dean, Mead, Egerton, Bloodworth, Capouano & Bozarth, P.A.
800 North Magnolia Avenue, Suite 1500
P.O. Box 2346 (ZIP 32802-2346)
Orlando, FL 32803

407-841-1200
407-423-1831 Fax
www.deanmead.com

Attorneys and Counselors at Law
Orlando
Fort Pierce
Viera

NICHOLE M. MOONEY
407-428-5110
nmooney@deanmead.com

Are You Required to Implement an Identity Theft Prevention Program?

September 1, 2009

Effective January 1, 2008, the "Red Flag Rules" (the "Rules") delineates who must implement an Identity Theft Protection Program (a "Program") and how. The Rules apply to financial institutions and creditors. Though a seemingly limited group, your business may fall within the scope of the Rules.

The Rules require that certain businesses implement a Program designed to detect the warning signs ("red flags") of identity theft and mitigate the effects of identity theft. This little-known rule has caused a stir lately among businesses rushing to determine if they must comply before the approaching deadline. In fact, the scope of the rule has caused so much confusion that the Federal Trade Commission, the agency responsible for enforcing the Rules, has delayed compliance from January 1, 2008 until November 1, 2009. Until recently, it was unclear whether businesses like healthcare providers and law firms must comply. Now, it is apparent that the FTC intends for the Rules to reach both. Still other businesses have lingering questions. Should I comply? How do I comply? What should my Program look like? Although the FTC has provided some industry-specific guidance, other businesses are left guessing. The purpose of this article is to help you decide if your business must comply and briefly outline the basic requirements for your written Program.

To determine if your business is covered by the Rules, ask yourself two questions. First, is my business a financial institution or creditor? A "financial institution" includes banks, savings and loan associations, mutual savings banks, credit unions, or any other entity that holds a transaction account (a deposit account on which the depositor can make withdrawals). The definition of "creditor" is very broad and includes any business or organization that regularly provides goods or services and bills customers later. For example, the FTC considers utility companies and automobile dealers creditors.

If your business fits into either the definition of financial institution or creditor, then you should ask: Do I maintain covered accounts? A "covered account" is one used primarily for personal, family or household purposes that is designed to permit multiple payments or transactions. Examples include credit card accounts, mortgage or automobile loans, and checking accounts. A covered account is also any account that is subject to a reasonably foreseeable risk of identity theft. Examples include small business accounts or single transaction consumer accounts. In determining if your accounts are subject to a reasonably foreseeable risk of identity theft, you should consider the methods your business uses to open and access its accounts and whether your business has had any previous incidents of identity theft.

If you are (or may be) a financial institution or creditor with covered accounts, how do you comply with the Rules? What should your written Program look like? One size does not fit all when it comes to these Programs. Your Program will largely depend upon the size of your business and its potential risk of identity theft. While complex businesses with a high risk of identity theft in their operations might require a more comprehensive Program, smaller businesses with a low risk of identity theft may have a less comprehensive Program.

There are four elements of a Program. First, identify the red flags of identity theft that might occur most often in your particular business or industry. You should examine risk factors particular to your business or the way you conduct business. For example, a business that permits its customers to access their account information online would have different risk factors than a business that does not. Also consider how identity theft has impacted other businesses within your particular industry. The FTC has published a list of common red flags that you can consult.

The second step is to monitor your customers' accounts for the red flags identified in step one. The policies and procedures of your written Program should address how you will detect these red flags when you open new accounts or disclose existing customer information. For example, reasonable procedures include checking a drivers' license before disclosing personal information to a customer or asking "challenge" questions to identify the identity of a customer over the phone.

The third step is deciding how you will act once you have identified a red flag. You might monitor customer accounts for further signs of identity theft, notify law enforcement, or contact the customer. The final step is to periodically review your plan to reflect changes in the risk of identity theft to your customers. These changes might occur as a result of changes in the way you access customer accounts or changes in the structure of your business.

Whatever your program looks like, it must be approved by your board of directors or, if you do not have a board, a senior employee. The board or some other committee or senior official must be directly involved in the oversight, development, and implementation of your plan. You must train your staff to detect red flags and mitigate identity theft. Your staff must report to your board at least annually on your business's compliance with the plan.

For more information on the Red Flag Rules and how it impacts your business, contact Nichole Mooney at 407-428-5110.