



RED FLAGS RULE AND IDENTITY THEFT PREVENTION PROGRAMS

BY: ANDREW HOWLE

NEXSEN | PRUET

CORPORATE PRACTICE GROUP ALERT - MAY 2010

On June 1, 2010, the Federal Trade Commission (the “FTC”) will begin enforcement of the Red Flags Rule (the “Rule”)¹. The Rule was adopted pursuant to the Fair and Accurate Credit Transactions Act. The Rule applies to all banks and other financial institutions and to every “Creditor.” The term “Creditor” is defined in the Rule to include any business or entity that sells goods or services on open account where the purchaser can make deferred payments (other than by credit card) for those goods or services. According to a representative of the FTC, unless a business sells its goods or services only for cash, check or credit card charge, the business is a Creditor and must comply with the Rule.

A Creditor must first evaluate its customer accounts to determine if it has “Covered Accounts.” There are two types of Covered Accounts. The first is a “consumer account”, which is an account primarily for personal, family or household purposes and that involves or is designed to permit multiple payments or transactions. Examples of consumer accounts include, but are not limited to mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, savings accounts, and credit card accounts of a credit card issuer. The second type of Covered Account includes any other account for which there is a reasonably foreseeable risk to the customer, or to the safety and soundness of the Creditor, of identity theft. These risks include financial, operational, compliance, reputation or litigation risks. This second type of Covered Account applies to accounts that may be particularly vulnerable to identity theft, such as small business accounts, sole proprietorship accounts, and single transaction consumer accounts.

In determining whether a business has the second type of Covered Account, the business manager should consider the methods that the business uses to open its customer accounts; the methods that the business uses to access the accounts (such as remote access by internet or

telephone, which can be done by persons other than the account holder); and the business’ previous experience with identity theft.

If the business manager determines that the business does not offer or maintain either type of Covered Account, then the business need not implement an “Identity Theft Prevention Program.” Nevertheless, the business manager still must periodically reassess the business’ customer accounts to determine whether it then offers or maintains Covered Accounts.

If a business does offer or maintain Covered Accounts, it must develop and implement a written Identity Theft Prevention Program (“Program”) to detect, prevent and mitigate identity theft with respect to the Covered Accounts. The complexity of the Program will depend, in part, on the nature and scope of the business. However, regardless of complexity, the initial program must be approved by the board of directors, a committee of the board or, if the business does not have a board of directors, someone in senior management. Additionally, the Program should include the preparation of annual reports to evaluate, among other things, the effectiveness of the Program.

The FTC has detailed information posted on its website about the Red Flags Rule and creating Identity Theft Prevention Programs. To access this information, click [here](#). That website includes “A How-to Guide for Businesses,” and a basic “Do-It-Yourself Template for Businesses at Low Risk for Identity Theft”. For those Creditors whose Covered Accounts and operations provide relatively little risk of identity theft, the guide and template might be all that is needed to create an adequate Program. For those Creditors whose Covered Accounts and operations involve higher levels of risk of identity theft, a more comprehensive Program is needed.

¹ *Fighting Fraud with the Red Flags Rule, A How-To Guide for Businesses*, available at <http://www.ftc.gov/redflagsrule> (last visited Dec. 1, 2009).

If you have questions, please contact any one of our Corporate Attorneys listed below.

NORTH CAROLINA:

Bob Baynes	bbaynes@nexsenpruet.com	336.373.1600	Greensboro
Andrew Howle	ahowle@nexsenpruet.com	336.387.5145	Greensboro
Bob Hull	bhull@nexsenpruet.com	704.339.0304	Charlotte
Scott Jackson	sjackson@nexsenpruet.com	336.373.1600	Greensboro
Sam Whitt	swhitt@nexsenpruet.com	919.755.1800	Raleigh
Bill Wilcox	bwilcox@nexsenpruet.com	336.373.1600	Greensboro

SOUTH CAROLINA:

Mark Bender	mbender@nexsenpruet.com	803.771.8900	Columbia
Franklin Daniels	fdaniels@nexsenpruet.com	843.213.5403	Myrtle Beach
Andrew Dennis	adennis@nexsenpruet.com	843.720.1714	Charleston
Jones Dubose	jdubose@nexsenpruet.com	803.771.8900	Columbia
David Hawkins	dhawkins@nexsenpruet.com	843.577.9440	Charleston
Jay Hennig	jhennig@nexsenpruet.com	803.253.8202	Columbia
Chris King	cking@nexsenpruet.com	864.282.1132	Greenville
Mark Knight	mknight@nexsenpruet.com	803.253.8245	Columbia
Jeff Locker	jlocker@nexsenpruet.com	843.689.6277	Hilton Head
Ed Menzie	emenzie@nexsenpruet.com	803.771.8900	Columbia
Brian Price	bprice@nexsenpruet.com	864.370.2211	Greenville
George Scott	gscott@nexsenpruet.com	803.540.2137	Columbia
Joel Stoudenmire	jstoudenmire@nexsenpruet.com	864.370.2211	Greenville

