GREENSFELDER
ATTORNEYS AT LAW

CORPORATE CLIENT ALERT

IS YOUR BUSINESS READY FOR ENFORCEMENT OF THE "RED FLAGS" RULE?

2009

Each year, over 10 million individuals are victims of identity theft. In response, the U.S. government has passed a variety of legislation to protect the privacy and security of personal information. Most recently, regulators have adopted the Red Flags Rule, an extension of the Fair Credit and Transactions Act of 2003. Approximately 11 million U.S. businesses and organizations are subject to the Red Flags Rule. However, outside of the financial services industry, many of these businesses and organizations are unprepared, and risk not only non-compliance, but also the safety and integrity of their customers' personal information. If your business is subject to the Red Flags Rule, you will need to immediately develop and implement a written program to prevent, detect, and minimize the damage that can be caused by identity theft. Many regulatory agencies are already enforcing the Red Flags Rule, and the Federal Trade Commission (FTC) will begin to enforce the Red Flags Rule on August 1, 2009.

WHO NEEDS TO COMPLY WITH THE RED FLAGS RULE?

The Red Flags Rule applies not only to traditional financial institutions, but also to almost any business that provides goods or services without requiring its customers to pay up front. The FTC has identified **finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies** as entities that must comply with the Red Flags Rule. **Non-profit and government entities** such as **colleges and universities** that defer payment for goods or services can also be creditors. **Many franchisors, merchants, hospitals, doctors, dentists and other healthcare providers** will also be considered a creditor by the FTC.

The Red Flags Rule is based on a company's business activities rather than its industry or the type of information it collects. If your business or organization is a "financial institution" or "creditor" with "covered accounts," then the Red Flags Rule applies.

- A "financial institution" includes any state or national bank, state or federal savings and loan association, mutual savings bank, state or federal credit union or other entity with a "transaction account" that belongs to a consumer. Most of these institutions are regulated by federal bank regulatory agencies and the National Credit Union Administration (NCUA). Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold a consumer "transaction account." In either case, a "transaction account" is a deposit or other account from which the owner makes payments or transfers, which includes checking accounts, a negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

- A "creditor" is defined very broadly to include any entity that regularly (i) extends, renews, or continues credit; (ii) arranges for the extension, renewal, or continuation of credit; or (iii) is an assignee of any original creditor who is involved in the decision to extend, renew or continue credit. Accepting credit cards as payment does not in and of itself make an entity a creditor, but "credit" is defined to essentially include any transaction where payment is deferred until after the sale is made or service is provided. **As a result, if you allow your customers to "run a tab" or put purchases "on account" and bill them later, you are a creditor. If you arrange for the financing of goods and services, you are a creditor. If you are a debt collector that regularly negotiates the terms of the debt, you are a creditor.**

- A "covered account" is an account either (i) used mostly for personal, family or household purposes, and that involves multiple payments or transactions or (ii) for which there is a foreseeable risk of identity theft. The FTC has identified credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts and savings accounts as covered accounts.

If you are a financial institution or creditor with covered accounts, you must develop a written identity theft prevention program that prevents, detects and mitigates identity theft in connection with the opening of new accounts and the operation of existing ones. Creditors and Financial Institutions that are subject to oversight by the NCUA, the FDIC, the Federal Reserve Board, the Office of the Comptroller of Currency and the Office of Thrift Supervision need to work with their regulatory agency to ensure compliance. The FTC will oversee compliance by all other entities that must comply with the Red Flags Rule.

WHAT ARE "RED FLAGS"

"Red flags" are certain patterns, practices and activities that are warning signs of identity theft. Red Flags fall into several broad categories:

- alerts, notifications or warnings from a consumer reporting agency;
- suspicious documents;
- suspicious personally identifying information (suspicious addresses, etc.);
- unusual use of, or suspicious activity relating to, a covered account; and
- notices from customers, victims of identity theft, law enforcement authorities or other business about potential identity theft related to covered accounts.

Specific examples of red flags include unusual account activity, fraud alerts on a consumer report, documents that seem to be altered or forged, and a suspicious account application document. On its Web site and in advisory opinion letters, the FTC has provided additional examples of possible red flags that must be considered when developing an identity theft prevention program

HOW DO YOU COMPLY WITH THE RED FLAGS RULE?

The Red Flags Rule does not proscribe a one-size-fits-all approach for combating identity theft. It permits the creation of a program that is appropriate for the size and complexity of your business. However, your program must reasonably detail certain policies and procedures that will prevent and mitigate identity theft. Therefore, your program must include:

- **Identification of Relevant Red Flags.** The program must identify patterns, practices and specific activities that indicate the possible existence of Red Flags. You should examine the methods used to open accounts, methods you provide to access accounts, and your business' previous experiences with identity theft. Examples of variables to consider are: does your business require identification or verification of identity when opening an account; does your business run a credit report or other third party verification; is there a time delay between opening an account and customer's receipt of goods or services; are the transactions in person, by mail, over the telephone or via a website; and does your business allow users to access their account by automated telephone systems or over the Internet?

- **Detection of Red Flags.** After the applicable Red Flags have been identified for your particular business, you must develop an approach to detect the warning signs of identity theft. Each business' approach to detecting Red Flags may be different depending on the size of the organization, nature of the business and type of accounts maintained.

- **Prevention and Mitigation of Identity Theft.** When potential identity theft is detected, an appropriate response is necessary. The response should be appropriate for the degree of risk, and may include: monitoring a covered account for evidence of identity theft; contacting the customer; changing passwords, security codes or other security devices that permit access to a covered account; reopening a covered account with a new account number; not opening a new account; closing an existing covered account; not attempting to collect on a covered account or not selling a covered account to a debt collector; notifying law enforcement; or determining that no response is warranted under the particular circumstances.

- **Periodic Updates to Ensure Continued Compliance.** As perpetrators of identity theft become more sophisticated, the methods for preventing, detecting and minimizing the damage caused by identity theft also are constantly evolving. To keep up with these changes, a periodic review of your business' identity theft program will be required. The review should begin with a reevaluation of what constitute "Red Flags" for your business, and should take into account your experiences with identity theft, any changes in the methods of identity theft, any changes in mitigating identity theft, changes in the types of accounts your business maintains, and changes in your business' structure or operations.

In addition, any business that issues credit or debit cards must create policies and procedures that assess the validity of a change of address request from its customers. Moreover, users of consumer credit reports must enact procedures to resolve address discrepancies from credit reporting agencies. As a result, your business must reasonably believe that a consumer report relates to the consumer for whom the report was requested in order to comply with the Red Flags Rule.

Finally, your program must be approved and managed by your Board of Directors (or its equivalent), provide for staff training so that employees are adequately prepared to comply with the Red Flags Rule, and include a plan for oversight of any service providers.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Consumers may seek actual damages, recover attorneys' fees and obtain punitive damages where appropriate. FTC penalties for non-compliance range from $3,500 to $16,000 per violation and could result in ongoing FTC audits. States may also enforce the Red Flags Rule on behalf of their citizens through direct damages or up to $1,000 per violation, plus the recovery of attorneys' fees. There are no criminal penalties for failure to comply at this time.

HOW GREENSFELDER, HEMKER & GALE, P.C. CAN HELP

Greensfelder, Hemker & Gale, P.C. has extensive experience advising clients on privacy, information security and identity theft. The attorneys in our Regulatory Compliance and Technology Transactions Practice Groups can assist in developing a program that complies with the Red Flags Rule, and integrating this program with your company's overall strategy for information security, vendor oversight and regulatory compliance.

Vince Garozzo
(314) 516-2624
vjg@greensfelder.com

M. Spencer Garland
(314) 516-2613
msg@greensfelder.com

Jason Ross
(314) 345-4754
jlr@greensfelder.com

Kevin Lux
(314) 516-2635
kjl@greensfelder.com

Zach Hammerman
(314) 345-4773
zlh@greensfelder.com

David Guard
(314) 335-6845
dsg@greensfelder.com

This Client Alert was prepared as general information to be given to our clients, contacts and friends. It is not intended, nor shall it be deemed, to constitute legal advice with respect to any of the matters set forth herein, and should in no event be acted upon without professional counsel. This material may be considered advertising under certain rules of professional conduct.

This document offers opinions of an informative nature and should not be considered as legal advice to any specific matter. © 2009 Greensfelder, Hemker & Gale, P.C. All Rights Reserved