What you need to know about the Red Flags Rule - Identity Theft Protection Programs

by Lewis Baum and Ken Cookson

Earlier this summer, in a Washington, D.C. coffee shop, a thief stole the purse of the wife of the Chairman of the Federal Reserve. With the information from the purse, the thief and/or others attempted to fraudulently obtain goods and services and made Ben Bernanke another victim of identity theft. That story, widely reported in the press, shows how much of an epidemic identity theft has become. With a man of such stature, who also sits on the President's Identity Theft Task Force, falling victim – it would appear that no one is immune. Recent press reports show that at least five persons have been prosecuted for having been part of that identity theft ring.

Identity theft has been reported as the fastest growing crime. There are many causes including the rise in methamphetamines and other drugs, and financial hardship. Clearly, an identity equals cash. Stealing an identity is relatively easy and seems like a "harmless crime." According to some surveys, such thefts cost individuals $850 - $1,400 in out-of-pocket costs with lost wages ranging from between $2,000 - $14,000. One of the fastest areas of identity theft relates to health care. Besides having similar costs and damage associated to your credit history, medical identity theft can cause a change in your medical records, which could potentially impact your employment or worse, kill you (among other less severe outcomes).

In response to this growing "epidemic," the U.S. Government has pushed to make combating identity theft a higher priority. This article will focus on the Red Flags Rule.

On November 1, 2009, after several delays, the Federal Trade Commission's ("FTC") Red Flags Rule will go into effect for businesses, non-profits and professional organizations. They apply to "financial institutions" and "creditors" (covered organizations) with "covered accounts" and should be designed to identify, respond to and protect against identity theft.

What is a covered organization?

The FTC's website, www.ftc.gov, contains helpful information for covered entities. There is a link to a guide, titled *Fighting Fraud with the Red Flags Rule: A How-to Guide for Businesses* which can help a covered entity determine whether an organization is at high risk or low risk for identity theft. The FTC has also issued a Do-It-Yourself Prevention Program and a list of FAQ's which will help a covered entity determine whether it is at low risk or high risk for identity theft.

For example, simply accepting credit cards as a form of payment does not make a business a "creditor" under the Red Flags Rule. Offering a company's own credit card, arranging for credit for customers or extending credit by selling customers goods or services now and billing them later, is more likely to make one a "creditor."

The Red Flags Rule does not require that the ITPPs be mailed to customers, as is the case with certain "privacy" policies. Further, there is no requirement for any form of notification outside of one's organization.

What is a covered account?

A covered account is a continuing relationship established by a person with a creditor to obtain a product or service for personal, household or business purpose. Such accounts are designed to permit multiple payments or transactions. The Red Flags rule also specifies that a covered account is any account for which there is a reasonably foreseeable risk from identity theft.

What does this mean to me?

The Red Flags Rule require that covered organizations with covered accounts establish Identity Theft Prevention Programs ("ITPPs") designed to prevent, detect and mitigate identity theft. The ITPPs should be uniquely tailored to each covered entity's size, complexity and nature of operations. Each ITPP should have the following four (4) essential features:

1. **Identify.** Each covered entity must identify and incorporate into its ITPP relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft. Depending on the nature of business operations, each covered entity's red flags will vary. The Rules require that the identity patterns be based on the guidance provided by the FTC as well as the covered entity's own experiences.

2. **Detect.** The ITPP should specify procedures for detecting red flags. The FTC's guidelines recommend obtaining and identifying information about, and verifying the identity of, persons opening new accounts, and in the case of existing accounts, authenticating customers, monitoring transactions and verifying address change requests.

3. **Respond.** Each ITPP must have policy provisions for responding to red flags that are detected to prevent and mitigate identity theft. Policies should include measures such as monitoring an account for evidence of identity theft, contacting customers who may be affected, notifying law enforcement agencies, changing passwords or other devices that restrict account access, freezing or closing the account, etc.

4. **Administer.** The ITPP must update its program periodically to reflect changes in risks as changes to identity theft occur.

The ITPP is required to be enacted by the Board of Directors of the covered entity as well as designating a person to be in charge.

Where does this regulation come from?

In 2003, Congress enacted the Fair and Accurate Credit Transaction Act ("FACTA"), which is codified at 15 U.S.C. § 1681-1681x. FACTA codified a number of measures intended to improve the accuracy of credit transactions and to curb identity theft and included an entitlement for each American to receive one free annual credit report. Section 114 of FACTA, 15 U.S.C. § 1681m, directed the FTC and other agencies to issue guidelines regarding identity theft. FACTA incorporated the definitions of "credit" and "creditor" from the Equal Credit Opportunity Act ("ECOA"), 15 U.S.C. § 1681a(r)(5).

"Credit" is defined under ECOA as the "right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefore." 15 U.S.C. § 1691 a(d). "Creditor" is defined in the ECOA as "any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit." 15 U.S.C. § 1691a(e).

On November 9, 2007, after preliminary drafts, the FTC, together with several other executive agencies, joined the issued final rules to implement FACTA. The rules are codified at 72 Fed. Reg. 63,718 (Nov. 9, 2007) now codified at 16 C.F.R. ~ 681.2.

Since the Red Flags Rules arise under FACTA and other legislation, and not the Federal Trade Act, jurisdiction extends beyond those covered under the Federal Trade Act and covers for-profit entities, non-profit organizations, and professional practices with covered accounts.

What should an ITPP look like?

Each covered entities' Red Flags Rule should be designed around the practical and experiential business of the covered entity. For example, the ITPP should recognize and respond to any changes in credit reports for customers' credit activity that may indicate identity theft. Likewise it should recognize when a fraud or an active duty alert on a credit report is noted, and notice of a credit freeze is reported, notice of the address discrepancy is provided, or a credit report is issued indicating a pattern of activity inconsistent with the account or the person's history, such as large increases in volume or credit inquiries. Likewise, suspicious documents should be identified. Suspicious documents that should trigger red flags include identification documents that it would appear altered or forged, the person presenting the identification doesn't match the photo or the physical description, the information on the identification differs from what the person presenting the identification has told you and credit applications appear to be altered, forged or somehow modified.

Examples of suspicious personal identifying information include:

-inconsistencies with what is already known about the customer, inconsistencies in the information the customer has given
-addresses, phone numbers or other information that is known to be fraudulent
-bogus addresses
-addresses to mail drops or prisons
-invalid phone numbers or social security numbers
-addresses or telephone numbers that have been used by other people for opening accounts
-the inability of a person to provide authenticating information beyond what basic information is available from a loan or a credit report, such as answering challenge questions

The ITPP should also take into account what the covered entity would do when notified of a change of address, requested to provide new or additional credit cards, asked to add users to the account, asked to handle an existing account that has been used for fraud or an account that is used in ways inconsistent with its account history, asked to handle long dormant accounts that are suddenly reactivated, returned mail to customers, and information about unauthorized charges to an account.

What to Do Going Forward?

For many businesses, their existing "loss prevention policies" will form the foundation for a more expansive Red Flags Rule ITPP. There is, however, no substitute for each covered entity analyzing the situation that it has and addressing the risks with appropriate policies. Further, the ITPP should be a living program. It should be revisited in a timely manner in order to consider and reflect new and changing threats. Such threats would include experience, training, societal, and industry specific considerations. While there is no private right of action to enforce the Red Flags Rules, either the FTC or the states' Attorneys General may seek enforcement and civil penalties can be imposed, but not criminal, and a "knowing violation" can result in a fine of $3,500 per incident. Being that many identity thefts occur through stealing of "chunks of data," the fines could quickly add up.

Lewis M. Baum, CPA/ABV/CFF, CVA, CFE specializes in Litigation Consulting and is with SS&G Financial Services, Inc. and can be reached at 440-248-8787 or by email at LBaum@SSandG.com

Ken Cookson practices law in Columbus with Kegler Brown Hill & Ritter. He can be reached at 614-462-5400 or kcookson@keglerbrown.com.