FTC Red Flags Rule—Protecting Against Identity Theft

By Marc L. Hamroff and Terese L. Arenth

IDENTITY THEFT, WHEREBY THIEVES use people's personally identifying information to open new accounts and misuse existing accounts, is a growing problem. Following the Fair and Accurate Credit Transactions Act of 2003 (16 CFR §681.2), the Federal Trade Commission (FTC), working with other federal agencies including federal bank regulatory agencies and the National Credit Union Administration, issued regulations, known collectively as the "Red Flags Rule," which require financial institutions and creditors to develop and implement written programs to prevent identity theft. The programs must identify, detect, and respond to warning signs, or "red flags," that could indicate identity theft.

Who Must Comply?

The Red Flags Rule applies to all "financial institutions" and "creditors" with "covered accounts." Under the rule, a "financial institution" is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other person that, directly or indirectly, holds a transaction account belonging to a consumer. See 16 CFR §681.2(b)(7) and 15 USC 1681a(t). Examples of financial institutions under the FTC's jurisdiction include state-chartered credit unions and institutions that offer accounts where the consumer can make payments or transfers to third parties.

The Red Flags Rule more broadly defines a "creditor" to include any person or business that arranges for the extension, renewal, or continuation of credit and includes all businesses or organizations that regularly permit deferred payments for goods or services. See 16 CFR §681.2(b)(5) and 15 USC 1681a(r)(5). Under this broad definition, a "creditor" encompasses commercial transactions, and not only are credit card companies and financial institutions subject to the rule but also automobile dealers, finance companies, and any other company that regularly extends or merely arranges for the extension of credit or makes credit decisions. The definition also includes any company that regularly participates in the decision to extend, renew, or continue credit, including setting the terms of credit. Given the breadth of the "creditor" definition, the Red Flags Rule arguably applies to businesses ranging from utilities and telecommunications companies to health care providers, lawyers, accountants, and other professionals. Presumably, it could also apply to equipment lessors and lenders, as well as other players in the equipment leasing industry who are in any way involved or participate in the extension of credit or renegotiation of credit terms or merely credit decisions.

The breadth of the rule's definition of "creditor," along with lack of guidance from the FTC, has created confusion and uncertainty in some industries as to their coverage under the rule and has resulted in the FTC's repeated delay in its enforcement. The FTC has been

accused of applying the rule to entities that were not intended by Congress to be encompassed by the definition of creditor, and recently, the American Bar Association brought suit in the U.S. District Court for the District of Columbia challenging the FTC's broad application of the rule and was granted an order barring the FTC from forcing rule compliance by attorneys and law firms.

Once a business has concluded that it is a financial institution or creditor, it must determine if it has any covered accounts. "Covered accounts" encompass both existing and new accounts and fall into two categories. See 16 CFR §681.2(b)(3). The first category is a consumer account that is offered to a company's customers primarily for personal, family, or household purposes and involves or is designed to permit multiple payments or transactions. Examples include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. The second category is "any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks." Examples provided by the FTC include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be particularly vulnerable to identity theft. The FTC examples, however, do not provide any guidance as to what may constitute a "small" business account and could open the door to an inference that accounts with large businesses do not fall within this category of covered accounts. However tempting that inference may be, the FTC has given indication that the size of the account or creditor is not the determinative factor. Rather, the key factor in determining whether an account falls into the second category is if the risk of identity theft is "reasonably foreseeable." To make this determination, it is necessary to take into consideration how the account is opened and accessed. For example, if an account can be accessed remotely by telephone or Internet there may be a reasonably foreseeable risk of identity theft, regardless of whether the account is with a small business, sole proprietor, or large corporation. Whether or not a business finance lease, for example, may be a covered account will turn on whether it presents a reasonably foreseeable risk of identity theft.

How to Comply

Companies subject to the Red Flags Rule ("covered companies") are required to design and implement a written identity theft prevention program, which must be designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones. The program must be uniquely tailored to a covered company's size, complexity of business, and the nature and scope of its activities. The height of a covered company's identity theft risk or the variety of covered accounts that it may have could impact its need for a program more comprehensive than the program of a company with lesser risk or covered accounts.

(1) Identify the Relevant Red Flags

According to the FTC, "red flags" are potential patterns, practices, or specific activities that indicate the possibility of identity theft. See 16

CFR §681.2(b)(9). Different kinds of risk may be associated with different kinds of accounts. Therefore, in identifying the relevant red flags, a covered company should take into consideration the types of accounts that it offers or maintains, the methods used to open covered accounts, how access is provided to those accounts, and the company's previous experience with identity theft.

To further aid in the identification of red flags, a covered company may consider other sources of information as a resource. Other sources may include, where available, the experience of other members in the company's industry (perhaps available, for example, from news or industry reports, or from "talk on the street" between industry members). Another source is consideration of how identity theft may have previously affected the covered company's business, as past experience could aid in identifying patterns, practices, or specific activities that indicate the possibility of identity theft.

Supplement A to the Red Flags Rule lists five categories of common red flags that a covered company should consider for inclusion in their program, as appropriate to that company's business: (1) alerts, notifications, or other warnings received from a credit reporting company (for example, an address discrepancy provided by a credit reporting agency or a fraud alert on a credit report); (2) the presentation of suspicious documents (for example, identification of applications that look forged); (3) suspicious personal identifying information (for example, a bogus address or inconsistencies with available information); (4) suspicious account activity (for example, an inactive account is suddenly in use); and (5) notice from other sources, such as a customer, a victim of identity theft, or law enforcement authorities.

(2) Detect Red Flags

Once a covered company has identified the red flags of identity theft for its business, the company's program must address the procedures and policies for detecting these red flags in the company's day-to-day operations. When verifying a person's identity when opening a new account, reasonable procedures may include obtaining and verifying the person's name, address, and identification number or government-issued identification card, such as a driver's license or passport. For existing accounts, a company's program may include reasonable procedures to authenticate customers, monitor transactions, and verify the validity of change-of-address requests.

(3) Prevent and Mitigate Identity Theft

When a covered company has spotted a red flag, it should be prepared to respond appropriately. The Red Flags Rule does not require any specific practice or procedures for an "appropriate" response but rather gives a covered company the flexibility to tailor its program to the nature of its business and the risks it faces. As a practical matter, this flexibility may make it that much more difficult to respond "appropriately" without further guidance from the FTC. The appropriate response will depend upon the degree of risk posed and may need to accommodate other legal obligations that a covered company may be subject to (for example, the obligation to file a suspicious activity report (SAR) for those financial institutions and creditors that are subject to the SAR rules). The FTC guidelines in the Red Flags Rule offer illustrative examples of some appropriate responses, which include monitoring a covered account for evidence of identity theft; contacting the customer; changing passwords, security codes, or other ways to access a covered account; closing an existing account; reopening an account with a new account number; or notifying law enforcement. One or more of these options, or some other option altogether, may be the appropriate response depending upon the facts of each particular case.

(4) Update the Program

The Red Flags Rule requires periodic updates to a company's identity theft prevention program to ensure that it keeps current with identity theft risks, recognizing that new red flags may emerge as technology changes or identity thieves change tactics.

How to Administer Your Program

The Red Flags Rule also enumerates steps that a covered company must take to administer its program, including obtaining board approval, training of staff, ensuring oversight by the board or a senior management designee, and reporting on compliance, at least annually, to name a few.

The FTC has delayed enforcement of the Red Flags Rule from November 1, 2009, until June 1, 2010, to give creditors and financial institutions more time to develop and implement their compliance programs. Once enforcement begins, failure to comply with the Red Flags Rule could result in civil monetary fines and lawsuits, so it is important that covered entities make a good faith, reasonable effort to comply. Enforcement of the rule can only be done by federal and state government agencies that are authorized by statute, including the FTC. The FTC, for example, can file a complaint against a noncompliant entity that seeks both monetary and civil penalties as well as injunctive relief for violation of the rule. In a situation where the complaint seeks civil penalties, the lawsuit is typically filed in federal court by the U.S. Department of Justice on behalf of the FTC. The maximum civil penalty per violation is currently $3,500, and each instance in which the company has violated the rule is a separate violation. Injunctive relief may require the parties being sued to comply with the law in the future, in addition to providing reports, retaining documents, and taking other steps to ensure compliance with both the rule and court order. Failure to comply with the court order could subject the parties to further penalties and injunctive relief. While there is no private right of action by consumers under the rule, consumers can file a complaint with the FTC about a company's program, and the FTC may use such complaints to target its law enforcement efforts. ■

ELT thanks Marc L. Hamroff and Terese L. Arenth, partners with Moritt, Hock, Hamroff & Horowitz, LLP.