Agencies Release FAQs on Identity Theft, "Red Flags," Change of Address, and Address Discrepancies Under the FACT Act

DAVID E. TEITELBAUM, MICHAEL F. McENENEY, JAMES A. HUIZINGA, KARL F. KAUFMANN, AND JOHN K. VAN DE WEERT

Recently, several agencies released guidance in the form of "FAQs" to address certain recurring questions regarding compliance with the identity theft and red flags rules, card issuer rules regarding change of address, and address discrepancy rules implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003. This article provides an overview of this guidance.

On June 11, 2009, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the Federal Trade Commission (FTC) (collectively, the Agencies) released a set of Frequently Asked Questions (FAQs) to address certain recurring questions regarding compliance with the identity theft and red flags rules (Red Flags Rules), card issuer rules regarding change of address (Card Issuer Rules), and address discrepancy rules (Address Discrepancy Rules) implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003

The authors are attorneys at Sidley Austin, LLP. They may be contacted at dteitelbaum@sidley.com, mmceneney@sidley.com, jhuizinga@sidley.com, kkaufmann@sidley.com, and jvandeweert@sidley.com, respectively.

Published in the August 2009 issue
of Privacy & Data Security Law Journal.

(FACT Act). While the FTC joined the other agencies in issuing these FAQs, the FTC indicates that it will be promulgating additional FAQs with respect to entities subject to its jurisdiction.

GENERAL RECORD RETENTION REQUIREMENTS

The FAQs caution that although none of the rules contains specific record retention requirements, entities subject to the rules still must be able to demonstrate compliance, apparently creating a *de facto* record retention requirement.

RED FLAGS RULES

Applicability

The Red Flags Rules apply to "financial institutions" and "creditors." "Financial Institutions" are defined as (1) all banks, savings associations, and credit unions, regardless of whether they hold a consumer transaction account, and (2) any other person that directly or indirectly holds a consumer transaction account. The Agencies have clarified that this means that all banks, savings associations and credit unions (including corporate credit unions) are subject to the Red Flags Rules, regardless of whether they hold consumer transaction accounts or are restricted to performing trust activities. Credit union service organizations are only covered to the extent that they meet the definition of "creditor."[1]

"Functionally regulated subsidiaries" of insured depository institutions are subject to the Red Flags Rules issued by the FTC, rather than the rules issued by the agencies that regulate their parent banks and thrifts. The FAQs confirm that a "functionally regulated subsidiary" for this purpose is defined in Section 5(c)(5) of the Bank Holding Company Act of 1956 (as amended by the Gramm-Leach-Bliley Act, 12 U.S.C. § 1844(c)), as any company that is not a bank holding company or depository institution and that is:

1. A broker or dealer that is registered under the Securities Exchange Act of 1934;

2. A registered investment advisor that is registered with either the Securities and Exchange Commission (SEC) or any state (with respect to the investment advisory activities of such entity and any activities incidental thereto);
3. An investment company that is registered under the Investment Company Act of 1940;
4. An insurance company that is subject to state insurance regulator supervision; and
5. An entity that is regulated by the Commodity Futures Trading Commission.

Thus, securities brokers, dealers, investment advisors, and insurance companies that qualify as "financial institutions" or "creditors" are subject to the Red Flags Rules issued by the FTC, even if they are subsidiaries of banks. Although this regulatory division of labor had been generally understood, the FAQs further clarify that these SEC-regulated entities are subject to the FTC's Red Flags Rules.

The Red Flags Rules do not apply to foreign branches of U.S. banks, although institutions are still urged to implement effective identity theft prevention programs without respect to such operations.

Covered Account

The Red Flags Rules define a "covered account" as (1) "an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions," or (2) "any other account that the 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."[2] The FAQs state that an account that meets either of the two parts of the "covered account" definition is considered to be a covered account and must be addressed by the entity's Identity Theft Prevention Program (ID Program). Such accounts include all consumer accounts established in the U.S., regard-

less of whether they are established by U.S. residents or non-U.S. residents. Whether an account meets the second part of the definition should be based on a risk evaluation that includes consideration of the methods the entity provides to open its accounts, the access methods it provides for such accounts, and any previous experience with identity theft.

The FAQs stress that the two parts of the "covered account" definition can apply broadly, depending upon the circumstances of the product in question. For example, the FAQs list leases, certificates of deposit, individual retirement accounts, trust accounts, business accounts, and small business loans guaranteed by consumers as products or arrangements that can fall under the definition of "covered account" if the terms of such products are covered by either of the two prongs of the definition. In this regard, certificates of deposit, individual retirement accounts, and trust accounts all are considered "accounts" that may satisfy the first part of the definition of "covered account" if they are for consumer purposes and permit multiple payments or transactions, and if not, would still need to be evaluated under the "reasonably foreseeable risk" test. The guarantee of a small business loan is considered by the Agencies to constitute an extension of business credit subject to the "reasonably foreseeable risk" analysis.

With respect to pre-paid cards, the FAQs provide additional, but incomplete, guidance. On one hand, the FAQs state that gift cards "issued without the creation of any record of the person who obtains the card, or the recipient of the card" would not be "accounts." Thus, anonymous gift cards appear to be excluded from the Red Flags Rules. On the other hand, consumer pre-paid cards that "permit multiple transactions and create a continuing relationship between the person who obtains and/or uses the pre-paid card and the financial institution that issues the card," such as payroll cards, are "covered accounts." Whether the Red Flags Rules apply to other types of pre-paid products that are identified to individual cardholders but is non-reloadable is not addressed by the FAQs.

The FAQs also address transfers of covered accounts, such as certain consumer loans. Although the entity that initially extends credit with respect to a covered account is responsible for applying its ID Program to the account's opening, any purchaser of such an account would then

become responsible for applying its ID Program to the loan as a covered account of the purchaser. The FAQs do not address whether this transfer interpretation applies only to whole loan transfers and not to mere sales of participation interests or receivables where the customer relationship is retained by the seller.

Identity Theft

The FAQs indicate that the creation of a fictitious identity using any single piece of information belonging to a real person, such as through check forgery, or use of a stolen credit card, constitutes "identity theft" for purposes of the rules.

ID Program Education

The FAQs encourage, but do not require, financial institutions and creditors to educate consumers about the prevention of identity theft.

ID Program Automation

The FAQs clarify that under the Red Flags Rules, financial institutions and creditors may use automated solutions to detect red flags, but are not required to do so. However, the FAQs caution that financial institutions may need to supplement an automated system with non-automated policies and procedures to ensure effectiveness.

Specific Red Flags Responses

According to the FAQs, the Red Flags Rules do not require any specific response to a particular red flag situation; examples provided in the Red Flags Rules are simply illustrative. As the FAQs state, the ID Program must simply include "policies and procedures for appropriately responding to identity theft that are commensurate with the degree of risk posed." Appropriate responses may include declining to open an account, filing a suspicious activity report, contacting law enforcement, and/or contacting the consumer.

Oversight of ID Programs

Financial institutions and creditors are required to engage in oversight of all service providers that perform activities in connection with the opening or accessing of covered accounts, not just service providers that offer fraud detection services. Such oversight need not be maintained through a specific written agreement, although the FAQs recognize that such agreements may be helpful. Service providers need not utilize the same ID Program as the financial institution or creditor they work with, so long as the ID Program they do utilize would be sufficient to meet the financial institution's or creditor's obligations under the Red Flags Rules.

Red Flags Examples

The FAQs reiterate that the examples of red flags provided in Supplement A to the Red Flags Guidelines are illustrative only, and that financial institutions and creditors may adopt some, all, or none of them, as they see fit.

CARD ISSUER RULES

U.S. Postal Service Change of Address Notices

Card issuers may not rely upon change of address notices from the U.S. Postal Service to meet their validation requirements. They must still utilize one of the address verification methods provided for in the Card Issuer Rules before honoring a request for an additional or replacement card that they have received within at least 30 days of also receiving a change of address notice from the U.S. Postal Service.

Corporate Credit and Debit Cards

The address verification requirements apply to corporate credit and debit cards that are in an individual employee's name and for which the employee is responsible for payment.

ADDRESS DISCREPANCY RULES

Applicability

The Address Discrepancy Rules apply only to notices of address discrepancy received from a nationwide consumer reporting agency (NCRA), either directly or from a third-party reseller or procurer acting on behalf of the NCRA.[3] However, the FAQs note that an address discrepancy notice received from a non-NCRA may still constitute a red flag for purposes of the Red Flags Rules. Notices that are received from third-party resellers or procurers are considered to be provided on behalf of an NCRA, and users of consumer reports are obligated to respond to those notices as if they had been received from the NCRA. However, if a consumer report does not indicate the NCRA from which the notice of address discrepancy was obtained, the user's policies and procedures would not need to require it to furnish confirmed addresses.

Reasonable Belief

In the event that a consumer withdraws an application to open a new account, a user who has received a notice of address discrepancy need not establish a reasonable belief that the consumer report relates to the consumer. However, if a user plans to deny a consumer's application to open a new account based on information in a consumer report, the user must take steps to ensure that the consumer report pertains to the consumer.

Furnishing Addresses to NCRAs

As the FAQs note, if a user receives a notice of address discrepancy from an NCRA, the user must have reasonable policies and procedures to provide the NCRA with the consumer's confirmed address if the user: (1) can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report, (2) establishes a continuing relationship with the consumer, and (3) regularly and in the ordinary course of business furnishes information to the NCRA that provided the notice of address discrepancy.

Published in the August 2009 issue
of Privacy & Data Security Law Journal.

A user is not required to use any particular mechanism to provide a confirmed address to an NCRA. Consequently, a user may, but is not required to, utilize specific reporting format codes adopted by the NCRAs with respect to confirmed addresses.

The FAQs clarify that whether a user regularly, and in the ordinary course of business, furnishes information to an NCRA, does not depend on the type or comprehensiveness of the information that the user regularly reports (e.g., only information regarding delinquent accounts). A user who only infrequently reports delinquent information, such as a small landlord who reports on delinquent tenants on an *ad hoc* basis, generally would not be considered to be reporting regularly and in the ordinary course of business, however.

NOTES

[1] "Creditor" is defined as a 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 C.F.R. § 1691a(e).

[2] The Red Flags Rules define "account" as "a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes."

[3] At this time, the only three NCRAs that the FAQs recognize are Experian, Equifax, and TransUnion.