



The new “red flag” rules under the U.S. Fair and Accurate Credit Transactions Act (FACTA) going into effect May 1 require U.S. banks and creditors to implement a program to identify, mitigate, and prevent potential consumer identity theft.

Will Red Flags Detour ID Theft?

Nikki Swartz

According to the U.S. Federal Trade Commission (FTC), consumers lose an estimated \$50 billion annually to identity theft and recovery expenses. During 2007, the FTC received 813,899 consumer fraud and identity theft complaints, an increase of 21% over 2006. The commission also estimates that losses to U.S. businesses and financial institutions stemming from identity theft total nearly \$53 billion annually.

The FTC hopes to reduce such losses with its Identity Theft Red Flag program, an update to the Fair and Accurate Credit Transactions Act (FACTA) of 2003. To meet the “red flag” requirements, all organizations that handle consumer credit accounts and transactions must conduct an identity theft assessment of their business and, based on those findings, develop measures to identify, mitigate, and prevent the theft of consumer data. The rules

also require organizations to update their programs periodically.

The FTC had originally ordered all creditors and financial institutions to comply by November 1, 2008. However, as the deadline approached, the majority was not prepared, and the FTC agreed to suspend enforcement until May 1, 2009. By that deadline, more than two million organizations must have a program in place to identify warning signs of a possible identity theft, along with defined responses to such incidents.

What Are the Red Flag Rules?

The red flag requirements issued by the FTC and five federal bank regulatory agencies apply specifically to Section 114 of the FACTA Identity Theft Red Flags and address retail and business customers, existing and new accounts, and financial institutions and creditors, including credit and debit

card issuers, among others.

The FTC said financial institutions and creditors who “offer or maintain covered accounts” must implement a red flag, or identity theft prevention, program. “Red flag rules apply to financial institutions and creditors like banks, credit unions, auto dealers, mortgage brokers, utility companies, and telecommunications companies,” an FTC spokesperson said.

Such companies must implement written programs – which must be in place by May 1 – to provide for the identification, detection, and response to patterns, practices, and specific activities, known as “red flags,” that could indicate identity theft for both new and existing accounts.

The FACTA final rules and guidelines implemented in Section 114 of the act lists 27 possible red flags that a business may use as starting points to formulate an identity theft program.

(See sidebar.) They fall into five categories:

1. Alerts, notifications, or warnings from a consumer reporting agency
2. Suspicious documents
3. Suspicious personally identifying information, such as a suspicious address
4. Unusual use of – or suspicious activity relating to – a covered account
5. Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts

According to *FTC.gov*, organizations' red flag programs must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the organization's board of directors or senior employees, include appropriate staff training, and provide for oversight of any service providers.

In simple terms, the red flag rules will force financial institutions to authenticate customers' identities, with the goal of spurring such organizations to better protect sensitive customer information.

Proponents say the rules will force financial institutions to be more diligent in analyzing consumer transactions and standardize how credit-issuing entities respond to suspicious activities regarding customer accounts.

Critics, however, argue that regulators have not provided guidelines on how to design such identity-theft programs, and the red flag rules just represent another burden for banks, which are already overburdened by current regulations.

Securing Customer Data

Still, no one argues that a program to stem the tide of identity theft incidents is not needed, especially not U.S. organizations. According to a study of

Red Flags

Six agencies were involved in drafting the new red flag rules: the Treasury Department's Office of Thrift Supervision, the Office of Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Trade Commission, the National Credit Union Administration, and the Federal Reserve System. They culled the following examples of red flags from the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003:

- A fraud alert included with a consumer report
- A notice of a credit freeze in response to a request for a consumer report
- A consumer reporting agency providing a notice of address discrepancy
- Unusual credit activity, such as an increased number of accounts or inquiries
- Documents provided for identification appearing altered or forged
- A photograph on ID inconsistent with appearance of customer
- Information on ID inconsistent with information provided by person opening account
- Information on ID, such as signature, inconsistent with information on file at financial institution
- An application appearing forged, altered, or destroyed and reassembled
- Information on ID not matching any address in the consumer report
- A Social Security number that has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased
- No correlation between the Social Security number range and the date of birth
- Personal identifying information associated with known fraud activity
- Suspicious addresses, such as a mail drop or prison, or phone numbers associated with pagers or an answering service
- A Social Security number matching that submitted by another person opening an account or by other customers
- An address or phone number matching that supplied by a large number of applicants
- The person opening the account unable to supply identifying information in response to notification that the application is incomplete
- Personal information inconsistent with information already on file at a financial institution or creditor
- Person opening account or customer unable to correctly answer challenge questions
- Shortly after a change of address, creditor receiving request for additional users of account
- Most of available credit used for cash advances, jewelry, or electronics, plus customer fails to make first payment
- A drastic change in payment patterns, use of available credit, or spending patterns
- An account that has been inactive for a lengthy time suddenly exhibiting unusual activity
- Mail sent to customer repeatedly returned as undeliverable despite continuing transactions on an active account
- A financial institution or creditor notified that a customer is not receiving paper account statements
- A financial institution or creditor notified of unauthorized charges or transactions on customer's account
- A financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft

Source: *Bankrate.com*

large U.S. organizations commissioned by Iron Mountain, the importance of protecting the access, destruction, and disposal of private or confidential information is a priority among business leaders because of the threat of identity theft.

According to “Compliant Information Destruction: Inside Corporate America Survey,” conducted between October 2007 and January 2008, nine in 10 organizations surveyed have a defined set of policies in place for safeguarding access to and the destruction and disposal of information. The survey polled business professionals and managers responsible for safeguarding information at companies with annual revenue of at least \$750 million.

For example, 54% of those who responded to the survey said their company’s leaders paid more attention over the past year to how their company destroyed and disposed of sensitive information. Thirty percent reported that their company increased its budget over the same time for in-

formation destruction and disposal.

Unfortunately, the survey also revealed that, despite those initiatives, many are unfamiliar with key federal and state laws governing information privacy, leaving them vulnerable to fines and data theft. While nearly three in four respondents (74%) said they were familiar with federal requirements, fewer than one in three (30%) said they were aware of the FACTA Disposal Rule, one of the foremost laws governing U.S. businesses on information security and disposal. This rule requires organizations to properly dispose of documents containing consumer information through methods such as burning, pulverizing, or shredding so the “information cannot practically be read or reconstructed.”

According to Iron Mountain, it’s not surprising that some companies seem unsure of the law. Over the past five years, myriad state and federal legislation has been enacted to protect sensitive consumer information. Cur-

More Information

The FTC has published a general alert on what the “red flag” rules require and an explanation of what types of entities are covered at www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

rently, 28 states have must-shred laws, and 43 have passed notification requirements for disclosing privacy breaches. U.S. federal laws include the Gramm Leach Bliley Act, the Fair Credit Reporting Act, and the Health Insurance Portability and Accountability Act. With each new law, companies must revise their policies and procedures for destroying information.

With the new red flag requirements, “The FTC is serving notice that it’s no longer enough for companies to simply say they have a policy for shredding or information destruction,” said Colleen Langevin, a vice president at Iron Mountain. “Now, organi-

zations must prove their policies and procedures actually work. Proving this means demonstrating good-faith efforts to document policies, train employees, audit behavior, and oversee service providers.”

Will New Rules End ID Theft?

According to experts, the red flag regulations are among the most important privacy initiatives in recent years. Other recent initiatives, they say, have left large holes in protecting against identity theft. They point out that other programs do not identify all the measures that financial institutions and creditors must take to identify and respond to questionable credit applications that are potentially created by criminals. The red flag regulations are intended to close these gaps, but can they prevent identity theft?

Red flag advocates say consumers will benefit from the higher standards required by the rules. For example, banks and creditors with sloppy fraud-prevention programs will eventually

be exposed by litigation and negative publicity. In addition, employees may become more vigilant in spotting identity fraud.

However, some creditors and financial institutions aren't happy about being forced to comply with more rules. Smaller institutions have complained that the rules will place an unnecessary financial and operational burden on them that they cannot afford. Many have said they may have to hire a third-party company to ensure compliance.

While the FTC informed financial institutions and creditors of the original November 1, 2008, deadline early last year, a recent BankInfoSecurity survey found that almost half of 300 surveyed institutions would have either barely met or would have missed the deadline.

While it may take time for institutions large and small to comply with the new requirements, no one denies they are necessary. The Iron Mountain survey revealed that there is much

room for improvement in protecting information. For example, its survey found that few (one in four or less) of the business leaders polled rated their company's initiatives related to employee training and education and compliance monitoring and reporting as "excellent." Furthermore, only 36% reported that their company currently conducts regular assessments of the risks associated with the disposal of private or confidential information. Less than one in four have a program reporting on compliant destruction of consumer information (24%).

But that presumably will change beginning May 1. What many are also hoping will change is the high number of identity theft incidents that occur each year. **END**

Nikki Swartz may be contacted at nikkiswartz@hotmail.com. See her bio on page 54.

See references for this article at www.arma.org/imm/jan09/redflag.pdf.