

Stopping Identity Theft

Fraud detection steps up front and center as the Red Flags Rule takes effect in August

By **Ted Dreyer**, senior attorney, Wolters Kluwer Financial Services

(ed. note: This article has been revised since appearing in the print edition of Scotsman Guide to reflect the delayed implementation date for the Red Flags Rule. On April 30, the Federal Trade Commission moved the date from May 1 to Aug. 1.)

AS OF AUG. 1, CREDITORS — INCLUDING mortgage brokers — must have a program in place to detect, prevent and mitigate identity theft. This requirement results from the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

The rule, whose implementation date recently was moved back from May 1 to allow more time for compliance, requires every mortgage broker who holds any covered account to develop and implement an identity-theft-prevention program.

Here's how to do so — and what you should know about FACTA's Red Flags Rule.



Federal banking regulators and the Federal Trade Commission (FTC) issued regulations implementing FACTA's Red Flags Rule with an original compliance date of Nov. 1, 2008. That date, however, turned out to be for depository institutions such as banks, savings associations and credit unions. Creditors that the FTC regulates, including mortgage lenders and brokers, received a six-month extension to May 1 to comply by developing their own programs; the FTC then moved the date to Aug. 1 to allow more time for compliance. Depository institutions already may have asked some mortgage lenders and brokers with which they do business to help meet their Red Flags Rule requirements.

To comply with the Red Flags Rule, there are



two categories of borrower accounts to consider.

1. Consumer accounts: The rule covers these accounts automatically if they are designed to permit multiple payments or transactions. These include mortgage loans and lines of credit.

2. All other accounts: These include commercial mortgages. To determine if nonconsumer accounts are covered, brokers must assess if the accounts have a foreseeable risk of identity theft. If they do, they must be covered.

Developing a program

As per the FTC, an effective identity-theft-prevention program must include reasonable policies and procedures for detecting, preventing and mitigating identity theft related to relevant accounts. It also must enable every financial institution or creditor to:

- **Identify relevant patterns, practices and specific types of activity considered to be red flags** — or signals of possible identity theft — and incorporate those red flags into the program;
- **Detect the red flags** that are incorporated in the program;
- **Respond appropriately to any detected red flags** to prevent and mitigate identity theft;
- **Ensure the program is updated periodically** to reflect changes in risks from identity theft.



Ted Dreyer is a senior attorney for Wolters Kluwer Financial Services in Minneapolis. Wolters Kluwer Financial Services is a leading provider of regulatory-compliance solutions for the financial-services industry. Reach Dreyer via e-mail at ted.dreyer@wolterskluwer.com or at (320) 240-5769. For more information about Wolters Kluwer Financial Services, visit www.WoltersKluwerFS.com.

Continued ...

REPRINTED FROM *SCOTSMAN GUIDE* RESIDENTIAL EDITION AND SCOTSMANGUIDE.COM, MAY 2009

All rights reserved. Third-party reproduction for redistribution is prohibited without contractual consent from Scotsman Publishing Inc.

Stopping Identity Theft

... Continued

The regulations include guidelines for developing a program, including illustrative examples of red flags. There are more than two-dozen examples of red flags divided into the following five groups:

1. Alerts, notifications or warnings from a consumer reporting agency
2. Suspicious documents
3. Suspicious personal-identification information
4. Unusual use of, or suspicious activity related to, the covered account
5. Notice from customers, victims of identity theft, law-enforcement authorities or other people regarding possible identity theft

Red flags that are relevant to each type of covered account should be included.

Determining relevance

In the mortgage industry, one of the most-important factors in determining which red flags are relevant is whether a customer relationship continues after origination or if the mortgage is sold. Lenders and brokers that maintain the relationship after origination must consider certain red flags that apply to continuing relationships. Those that do not only must address red flags that occur at origination.

Another important factor in determining which red flags are relevant is whether the mortgage disbursements only occur at closing or if additional advances can take place, such as those made as part of a home equity line of credit. Identity thieves are unlikely to hijack mortgages in which the proceeds are disbursed because there is no further financial incentive. The same cannot be said of loans that may result in additional advances.

There are many ways of detecting red flags, depending on the specific flag. Some lend themselves to the following manual-detection methods.

- **Review of a consumer report:** Brokers may be notified in the consumer report of a fraud alert, credit freeze or address discrepancy. They might need to notice a pattern of unusual account activity.

On the Web

- **Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 Final Rule:** bit.ly/redflag
- **Federal Trade Commission credit-regulation resources:** bit.ly/ftcstuff

- **Visual review of an identity document:** Several red flags involve a staff member looking at an identity document, such as a driver's license or passport, and detecting irregularities on it or comparing it to the applicant's appearance.

- **Review of an application:** Brokers may notice that the application appears to have irregularities or missing information.

- **Notice of unauthorized charges or identity theft:** This occurs when someone provides notice that a broker opened an account for a person engaged in identity theft.

Automated detection

Although manual detection of red flags is possible, several red flags lend themselves to an automated approach. These include the following.

- **Positive verification:** This type of customer verification ensures that information applicants provide matches information available from trusted-third-party sources. Automated systems can verify applicants' identities by comparing their application answers to information in a trusted database.

- **Negative verification:** This ensures that information provided has not been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine if any of the information is associated with known fraud incidents.

- **Logical verification:** This is a check on whether the information provided is logically consistent. For example, do the telephone number and street address match? People attempting identity theft often will provide some correct information but a false address or phone number so that the victim won't be contacted.

- **Customer authentication:** Usually, this is accomplished by asking challenge questions about an individual's past to verify identity. One red flag involves individuals who cannot provide information beyond what's available in a stolen wallet or consumer report. This can be accomplished manually or via an automated system.

Service-providers

The Red Flags Rule also mandates that financial institutions and creditors exercise appropriate and effective oversight of their service-provider arrangements. The regulation, however, provides little clarification as to what this really means.

Regulators' goal was to retain a flexible approach and to allow covered businesses to manage their relationships to serve their needs. For example, if a broker uses a service-provider to start a lending relationship, that would be the type of provider subject to the Red Flags Rule provision. In other cases, mortgage brokers might be the service-provider for another business covered by the Red Flags Rule. This would be the case in a wholesale-lending relationship.

The first step is obtaining contractual assurance that the provider has a program in place to detect red flags. This doesn't require that the provider comply with any specific program. Many providers serve multiple organizations, and it would be almost impossible to expect a provider to comply with multiple identity-theft programs.

A contract with a service-provider also should state that the provider will give notification of red flags or will take appropriate steps to handle red flags. It also should state that the provider attempt to prevent or mitigate any identity theft uncovered.

Brokers not only should be aware of red-flag requirements, but they also should understand that noncompliance could lead to large monetary penalties.

■ ■ ■

The strict protection of customer information is not something that mortgage brokers should take lightly. Failure to protect customer information adequately puts a broker's finances, reputation and business in jeopardy.

By understanding and complying with the Red Flags Rule, brokers can help stop identity theft and earn faithful clients at the same time. 