

ID Theft Red Flags Rule: How to Help Your Business Customers Comply

Auto Dealers, Mortgage Brokers, Utility Companies are Among Non-Banking Entities That Must Comply by Nov. 1

Linda McGlasson, Managing Editor
September 8, 2008

With all the focus on banks and credit unions' work to comply with the [ID Theft Red Flags Rule](#), many in the financial services industry have forgotten that the largest share of entities impacted by this new regulation are non-banking institutions -- finance companies, automobile dealers, mortgage brokers, etc.



And while banking institutions have their own hands full ensuring Red Flags compliance, they still can perform great customer service by assisting business customers who also must comply with the regulation.

The Red Flags Rule is part of the [Fair and Accurate Credit Transactions \(FACT\) Act of 2003](#). Under this rule, financial institutions and creditors with covered accounts must have identity theft prevention programs in place by November 1, 2008, to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Banking regulatory agencies are working with their institutions to ensure compliance. Meanwhile, the [Federal Trade Commission](#) oversees compliance by the rest of the covered entities identified as creditors.

Which Non-Banking Entities Must Comply?

The FTC has an extensive outreach effort to explain the Rule in greater detail. According to Tiffany George, attorney in FTC's Division of Privacy and Identity Protection, many companies that don't think of themselves as creditors or believe they need to create a prevention program for identity theft actually are deemed a covered entity under this rule.

These covered entities, no matter how small, need to design and implement an identity theft prevention program, George adds.

She reminds companies that the rule is not based on what kind of information a business collects, but whether it is a financial institution or a creditor. "A creditor is broadly described as anyone who defers payment on a debt, or anyone who defers payment on goods or services," George says.

Further, a creditor is:

Any entity that regularly extends, renews or continues credit;

Any entity that regularly arranges for the extension, renewal or continuation of credit;

Any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit.

Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors do include:

Finance companies,

Automobile dealers,

Mortgage brokers,

Utility companies,

Telecommunications companies.

Even healthcare providers who defer payment (provide credit) for patients also fall under the creditor status according to the rule. "Any interaction where a consumer is not paying up front would make the business a creditor," "So in the healthcare context, even where a consumer offers insurance (that would normally cover the bill), if the patient is still ultimately responsible for medical fees not covered by insurance, then that hospital or doctor's office would be considered a creditor," George explains.

Other examples of companies that would fall under the ID Theft Red Flag rule: Home improvement service companies that offer monthly repayment schedules for customers' home improvement projects such as siding, window replacement and remodeling.

"Entities need to realize this applies to anyone who defers payment for a good or service," George says. "Even mom and pop stores that offer monthly credit to customers would fall under this rule. Again, the nature of their program should be tailored to the nature of their business. If their business isn't complex, then they could have a very straightforward, streamlined program."

Where non-profit and government entities defer payment for goods or services, they, too, are considered creditors. Most creditors, except for those regulated by the federal bank regulatory agencies and the NCUA, are under the jurisdiction of the FTC.

The Requirements

Under the Red Flags Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs - or "red flags" - of identity theft. These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program 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 Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

Designing and putting in place a program that is appropriate to a creditor's size and complexity and nature of its business can be helped through the guidelines issued by the FTC and the federal banking agencies says George.

Businesses should be watching for the 26 possible red flags identified in the guidelines. These red flags should be used as a starting point by creditors and fall into five categories:

Notifications, alerts, or warnings from a consumer reporting agency;

Suspicious documents;

Suspicious personally identifying information, such as a suspicious address;

Unusual use of - or suspicious activity relating to - a covered account;

Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

The nature of a company's ID theft prevention program will vary based on a company's business, says George. "It will involve things such as proper identification

and authentication of customers; looking for anomalous activity in customer accounts; and looking for any suspicious or forged documentation," she notes.

If companies don't comply, enforcement outside of the banking industry will be done by the FTC. "We expect covered entities to be compliant by November 1," she says.

If they aren't, then they will be in violation of the rule and will be subject to civil monetary penalties of up to \$2500 for every violation. Violations will be considered on a case by case basis, says George.

[Close Window](#)

BankInfoSecurity.com is your source for bank information security news, regulations, and education.