



## **EXCLUSIVE: RULES THAT REQUIRE TIGHTER ID PROTECTIONS TOUCH COLLECTORS**

Posted by Mary Wisniewski on December 2, 2008 at 12:30pm

The compliance flavor du jour is to tighten up on identity fraud, because of the FACT Act Identity Theft Red Flags Rule. But what does the FACT Act mean for the collection industry?

The rule, issued by the FTC, the federal bank regulatory agencies and the National Credit Union Administration, requires creditors to establish written, identity-theft-prevention programs that "provide for the identification, detection and response to patterns, practices or specific activities – known as 'red flags' – that could indicate identity theft."

The deadline for implementation was slated for this month, but it was postponed until May 2009 "to provide creditors, financial institutions and service providers additional time to develop and implement written identity prevention programs." The extension of the rules does not affect other federal agencies' enforcement of the Nov. 1 deadline for subjects under their jurisdiction.

All creditors, from automobile dealers to mortgage companies, must comply with the Red Flag Rule – and they are not close to being ready, except for banks.

Ted Dreyer, senior attorney at Wolters Kluwer Financial Services, a vendor that sells compliance services, says depository institutions are "fairly well along" with setting up red flag procedures, but that does not mean all creditors are prepared. "Many of the automobile dealers [for example] might not even know they will be subject to this rule," he says.

### **NOT READY**

Avivah Litan, vice president and analyst at Gartner, says other than banks, many creditors are not red-flag ready. Litan says many companies are confused about a simple fact: is it a creditor or not?

"There is little awareness and little enforcement," Litan says, adding she is unsure whether an extension will ensure all creditors will be in compliance.

The rules might apply to third-party debt collectors, too. ACA International says although third-party collectors are excluded from the rule, some situations may require compliance.

"Debt collectors may be considered 'creditors' -- particularly in light of the commentary circulated in connection with the publication of the final rule last year," said Tomio Narita, Esq., of Simmonds & Narita LLP and ACA International's Members' Attorney Program Committee, in a news release. Narita also said third-party debt collectors may have to create an identity theft prevention program, even if they aren't considered creditors.

### **GET IN THE TECHNOLOGY GROOVE**

To get in compliance, vendors are offering technology solutions.

DealerTrack, provider of sales and on-demand software for the automotive retail industry, released a red flags tool as part of its compliance suite offerings earlier this year.

“Dealers should get on top of this,” says David Trinder, senior vice president of Network Solutions at DealerTrack, noting there are many dealers who still need to implement a red flag procedure.

All the same, many dealers do realize the importance of the compliance suite, as it is one of DealerTrack’s fastest selling items.

Dealers are certainly not the only niche getting red-flag technology offerings.

TransUnion is simplifying the compliance issue for the healthcare industry and recently updated the identity verification and authentication tool component parts of Revenue Manager, a TransUnion product.

## HOSPITAL FLAGS

TransUnion has more than 100 hospitals using its red-flag compliance technology and expects to exceed 120 by yearend, says Marty Callahan, vice president of TransUnion’s Healthcare Information Services.

Identity theft keeps on rising, given the bad economy, Callahan says and projects the crime to continue growing. “Hospitals need to pay attention to this issue,” he says.

Litan at Gartner recommends ID Analytics as an “innovative” red-flag technology tool. The solution itself detects and resolves red flags. For example, if a consumer gets a few flags on his or her account, the technology will generate “authenticating” questions, with an aim to resolve the flags. The solution uses an ID Network, which helps to keep false alarms at bay.

Todd Higginson, ID Analytic’s director of product remarketing, says the rules dictate that creditors must document red flags relevant to their business that indicate identity theft.

“Creditors aren’t afraid to comply,” he says. “The concern is the application requiring review will drive up costs and delays and introduce customer friction to the interaction.”

First California Bank, for example, is all set. The financial institution is using Compliance Pal’s red flag training program to prep for compliance. “I have been really pleased with their modules and training,” says Nanette Hutchison, senior vice president and certified regulatory compliance manager.

And it isn’t the only bank.

Gartner reported earlier this year that most financial institutions are up to the task.

“Compliance is still the main driver for fraud prevention and customer authentication projects, but 60% of surveyed banks already consider themselves to be compliant with the red flag regulations of the U.S. Fair and Accurate Credit Transactions Act of 2003,” said Gartner’s Litan in a July statement.

Even with policies in place, employees will determine how compliant a creditor is.

At First California Bank, the hardest part of staying compliant is getting its 250 employees to care about identity issues, Hutchison says. Even if employees do the training and pass the test, there are concerns that they might not follow the red flags because of indifference.