

ID Theft Red Flags: Institutions Found Lacking in Awareness, Vendor Management

FDIC Examiners Find 'Substantial Compliance' with New Reg, But Also See Common Challenges

Linda McGlasson, Managing Editor
March 31, 2009

In the five months since the compliance deadline for the Identity Theft Red Flags Rule, banking institutions generally are compliant. But examiners are finding issues with security awareness and vendor management.



This is the initial report from the Federal Deposit Insurance Corporation (FDIC), the largest U.S. bank regulator. The FDIC and other regulators have been testing Red Flags compliance at financial institutions since Nov. 1.

The good news, says Michael Jackson, spokesperson for the FDIC's regulatory compliance division, is that examiners have found "substantial compliance with the Red Flags regulations."

Still, there are three common issues that have arisen among banks that have been examined:

Covered Accounts - Some banks are misidentifying their covered accounts. Small business accounts are not automatically covered under the Red Flags regulation, Jackson says, but some should be included if the risk for identity theft is reasonably foreseeable. Some banks have had small business accounts that were victims of identity theft, but were not included among covered accounts.

Security Training - Some banks have not put together employee training, which is required, Jackson says. "By the regulation, they may have talked about it or assigned it to someone, but they need to have an actual program in place and have their employees trained on it." He says it would look better to examiners if institutions already had moved forward in training. "While banks may at this time be more focused on other things -- they may have [training] scheduled for sometime in the future -- but it is something they do need to work on a little more."

Vendor Management - Another area where examiners are interested in is in the area of third-party service providers (TSPs), says Jackson. "Banks are not adequately overseeing the oversight of their third party service providers' (TSP) compliance with red flags regulation," he says. "Even though they are not directly answerable to the regulation, these TSPs that hold information on these covered accounts or process transactions for these covered accounts need to be taking appropriate steps to prevent and mitigate ID theft."

Jackson notes that some institutions "are not taking appropriate action and are taking the word of the TSPs that they are meeting the requirements, or are assuming that they are not covered under the regulation. But banks should do a little due diligence and test them to make sure that they have these procedures in place."

Examinations: What to Expect

The FDIC wants to see movement toward substantial compliance with this regulation, Jackson says. "During the first year of examinations, we'll be looking for examples of banks that can represent the 'best

of breed' institution that has done a stellar job of meeting the requirements."

As the examiners so through these different regulatory exams, Jackson says, "We expect substantial compliance, and next go around we expect to see 100 percent compliance."

The FDIC and other examining bodies say they went through extensive outreach to financial institutions in advance of examinations. "There is no reason that a bank shouldn't have a program in place," Jackson says.

Coming soon from the FFIEC: A document compiling the most frequently asked questions about Red Flags compliance. "This FAQ should answer any questions that financial institutions have in a very specific way," Jackson says.

OCC Sees No Big Problems

The banks the Office of the Comptroller of the Currency (OCC) oversees can range from the very largest banks to those with less than \$250 million in assets.

"So far we've not seen a lot of problems," says Ann Jaedicke, Deputy Comptroller for Compliance Policy at the OCC. "But I want to couch that it is still early in the exam process; our examiners are still working their way through the banks."

To get a feel of how well OCC-regulated banks are doing in Red Flag compliance, Jaedicke pulled a sample of some of the exams, and says there were a few cases where the bank's board of directors had not approved the program. "While it is a pretty technical point, it is an important one. We want the board to approve the program."

In another case, she says examiners thought the bank needed to do a better job of identifying their covered accounts. Jaedicke notes the regulation specifies what a covered account is, but then adds, "And anything else you think needs to be covered under the identity theft program." She speculates that the accounts that the examiner referred to are under that "anything else" category. She recommends that banks "go through their product lines to see what lines may be more susceptible or where they've had identity theft problems in the past."

Jaedicke states the OCC did a lot of work prior to the date to get the banks ready for this compliance. "It is hard to measure how effective it was, but we did a lot of up-front work through examiners and other ways to get those banks started on a program of compliance. The longer we go without significant problems showing up, the more likely it is that all of the front work pays off."

Credit Union Exams Begin In April

The National Credit Union Administration's Examination and Insurance division says that it will begin reviewing credit union identity theft red flag programs starting with 2nd quarter 2009 examinations. "We anticipate red flags program information to start flowing soon," says the division's spokesperson. In March, NCUA officially released the examination procedures to its examiners.

In October 2008, NCUA released to credit unions the Interagency Identity Theft Red Flags Examination Procedures. "This release provided credit unions with an understanding of what our examiners would be reviewing on the credit union's red flags program," the NCUA says.

The NCUA recommends that credit unions should ensure they review NCUA Letter to Credit Unions 08-CU-24, NCUA Rules & Regulations Part 717, Subpart J (Identity Theft Red Flags) and Appendix J (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation). Credit unions should ensure their policies and procedures are updated, as necessary, to be in compliance with the regulation.

http://www.bankinfosecurity.com/articles.php?art_id=1327&rf=033109eb