



Western
Independent
Bankers

Directors Digest

A Community Bank Directors Advisor

Issue #15 - September 2008

Is Your Identity Theft Program Ready?

By Kevin K. Watson, AuditOne

Has your board reviewed and approved the Identity Theft Program that is required to be in place by November 1 of this year? The additional regulations to the Fair and Accurate Credit Transactions Act, or FACT Act, released November 9, 2007, require you to be in compliance by that date. While it remains to be seen how literally these new requirements will be applied by examiners, there is a great deal of momentum in that direction. The regulations explicitly require the program to be approved by the board or a board committee.

The increasing incidence of identity theft has caught the eye of our media and government, creating the momentum to do something big to resolve the problem. Being a heavily regulated industry as well as the engine and conduit for retail transactions, bankers can expect to carry the heavy load of the regulatory reaction.

The FACT Act itself is not new. It was originally passed in 2003 as an amendment and addition to the Fair Credit Reporting Act of 1970. It contained a variety of goodies for bank compliance officers, one of which was the requirement for the regulatory agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft. Those regulations will finally become effective this November. They concern both loan and deposit customers of the bank.

As a director, how can you carry out your explicit duty to ensure your institution has effectively implemented an identity theft program in compliance with the new regulations? Of course, the first step is to verify that responsibility has been assigned at the management level. Demand that the policy be received for review as soon as possible. There are four major elements the program must contain. Number one, it must identify the relevant red flags for your institutions. Examples of red flags are included in the appendix to the regulation. Some of them are universal, like receiving an alert from a consumer reporting agency or the presentation of suspicious documents by a prospective customer. If it is not obvious which red flags to adopt for your own, management can prepare a risk assessment in order to focus on those with the most likelihood or negative impact for your unique clientele and product offering.

The second element required to be decreed by policy, is how the red flags will be detected. In other words, which employees have the responsibility to be looking for red flags and how will they look. Thirdly, the policy must state how management and staff will respond when they see a red flag. For example, they might contact the customer or decline to open the account. Finally, the policy must contain a provision as to how it will be maintained up to date. One way to accomplish this is to provide for the maintenance of a risk assessment for identity theft, much like those maintained for BSA and information security. Sooner or later, it seems all regulatory risks will require a formal risk assessment. In addition to the required policy elements, the policy must also describe the identity theft training program for customer contact staff.

While, as a director you can't be an expert in all banking matters, there are certain things you must do, and one is to ensure regulatory policy minimums are met. You can gain comfort that your policy is adequate and is being effectively implemented by asking management for an annual report on the status of your identity theft program and by asking that your internal auditor review for compliance with the Identify Theft Regulations.

Kevin K. Watson is President of AuditOne, LLC (www.audit-one.com), a California-based independent internal audit firm specializing in banks and their service providers throughout the United States . Watson has 22 years of experience in the banking and auditing industries. He can be reached in AuditOne's Southern California office at 562-802-3581 or kevin.watson@audit-one.com.