



December 2005

COMMUNITY
BANKERS OF
CALIFORNIA

Published for members
and colleagues of
Community Bankers of California

Update

Warning: Compliance With The Bank Secrecy Act Is Serious Business

By: Jeffrey Huron of Huron Law Group

Today, the biggest concern for bankers is compliance with the Bank Secrecy Act ("BSA") as amended by the USA Patriot Act in 2001. The government's aggressive enforcement of the BSA has resulted in enormous take-notice penalties against several institutions including Riggs Bank (\$25 million), AmSouth Bank (\$50 million), and Banco de Chile (\$3 million).

Even the smallest community banks must comply with the BSA. Here are some **DO'S** and **DON'TS** when it comes to the BSA:

DO conduct a risk assessment. Your risk assessment should focus on customers with cash-intensive and frequent wire transfer activity. Implement and enforce policies and procedures that allow you to "know" the customer. Monitor account activity and make sure the cash transactions are in check with your records. **DO NOT** grant cash transaction report exemptions until you are certain the customer is legitimate.

DO train your employees. Training should emphasize how to detect and report suspicious activity. Training should not just include tellers and new account officers, but also commercial loan officers. Your loan officers should know how to look for signs of illegal activity, especially when they call upon their customers. Employees must also know how to communicate suspicious activity to management. Management must know how to report suspicious activity and BSA enforcement efforts to senior management, who, in turn, should report all of this information to the board. Pursuant to the BSA, senior management and the board are responsible for overseeing suspicious activity reporting and BSA compliance. Make sure you and your board **DO NOT** ignore these responsibilities.

DO file a Suspicious Activity Report ("SAR") for all suspicious activity. The SAR should identify the five essential elements of information: who? what? when? where? and why? Suspicious activity is defined broadly and includes suspicious activity: (1) that is "conducted through" your institution even if it occurred

elsewhere, (2) that does not result in a loss to your institution, and (3) that involves a false use of a taxpayer identification number. If the suspicious activity continues after you have reported it, **DO NOT** stop reporting the suspicious activity. **DO** pay special attention to subpoenas from law enforcement regarding a customer. This is a red flag that illegal activity may be occurring through your institution. You should immediately review the subpoenaed customer's account history and report any suspicious activity. Therefore, your subpoena compliance personnel must be trained to inform your BSA compliance personnel of all law enforcement subpoenas.

DO NOT ignore your employees. **DO** make sure that you have a system in place for addressing and documenting the handling of all internal suspicious activity reports.

DO conduct internal audits. These audits should include review of all banking activities and review those situations where suspicious activity was not reported. **DO** report the results to senior management and the board. Also, **DO** incorporate the results into your training.

Given the immense pressures on the government to limit terrorist activity, regulators are under strict marching orders to aggressively enforce the BSA at all levels. Therefore, all financial institutions must comply with the BSA or suffer serious consequences.


Happy Holidays
from
Community Bankers
of California 