In the aftermath of the terrorist attacks of September 11, 2001, President Bush signed into law the USA PATRIOT Act. With its lengthy official name, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, the Act covers a broad range of activities. Title III is the most important part of the Act for financial institutions, amending the Bank Secrecy Act as well as providing numerous provisions in the fight against international money laundering. The provisions, some of which are now in effect while others will follow on a rolling schedule, do not impose any new formal reporting obligations for banking organizations, but do require certain due-diligence, communication, and recordkeeping practices.

Make Bank Records Available

As of December 25, 2001, financial institutions must be able to produce bank records relating to anti-money-laundering compliance and customer accounts upon the request of federal regulators. While the previous regulations allowed financial institutions a “reasonable time” to produce such records, they are now given 120 hours maximum.

<table>
<thead>
<tr>
<th>Checklist 1</th>
<th>Bank Record Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>✑ Does the bank have the ability to produce requested documents?</td>
<td></td>
</tr>
<tr>
<td>✑ Is the production time less than or equal to 120 hours from time of request by the federal regulator?</td>
<td></td>
</tr>
<tr>
<td>✑ If not, proactive steps must be taken to increase the bank’s production capabilities.</td>
<td></td>
</tr>
</tbody>
</table>

The provisions of the USA PATRIOT Act are designed to enhance the ability of law enforcement and regulatory agencies to detect and prevent terrorist financing and other financial crimes. The Act requires financial institutions to adopt policies and procedures to detect and report suspicious activity, and to establish anti-money-laundering programs. The Act also provides legal authority for financial institutions to share information with other financial institutions and with law enforcement and regulatory agencies.

Community banks are introduced to sections of the USA PATRIOT Act of particular importance to them and are offered implementation checklists, in this article based on a presentation made at RMA’s 2002 Annual Conference.

Be Aware of the Safe Harbor

Under current law, financial institutions are protected from civil liability for reporting suspicious activity. The Act clarifies the coverage of this enacted safe harbor. The safe harbor does not apply if an action against the institution is brought by a government entity. In addition, the Act clearly prohibits bank employees from disclosing that a SAR (Suspicious Activity Report) was filed. Finally, a new clarification was made regarding employment references and terminations. If a bank is asked to give a reference about an employee who has been involved in suspicious activity, the bank may discuss only those suspicious events that occurred up to the time of termination.

© 2003 by RMA. Matt Schriner is the managing director of Financial Services and Lindsay Martinson is a risk management/compliance consultant with RSM McGladrey, Inc.
While the bank may disclose this information, it may not disclose that a SAR was filed. In light of these allowances, there is no protection for malicious disclosure. Therefore, your bank must use caution when asked to make these types of disclosures.

Check Your Anti-Money-Laundering Policy Focus
Since 1987, all federally insured depository institutions have been required by their federal regulators to have anti-money-laundering programs. The existing programs should contain the same elements required by section 352 of the Act. Your anti-money-laundering policy should demonstrate that your bank has implemented internal policies, procedures, and controls for the prevention of money laundering. It must also designate a compliance officer, provide personnel training guidelines, and indicate adequate independent testing is conducted. Currently, no specific guidelines offer banks a further breakdown of these four broad requirements. The most significant change in your money-laundering policy should be the overall structure and underlying attitude. Your policies and procedures should move from a strict BSA (Bank Secrecy Act of 1970) compliance focus to a more comprehensive, risk-based strategy to detect and report potential money laundering. Your bank can demonstrate this proactive approach by identifying and investigating high-risk accounts. Many banks have incorporated a list of business accounts they think may potentially be active in a money-laundering scheme. It acts as the bank’s “watchdog list.” Additionally, you may incorporate reports run for other purposes, such as suspect kite reports and demand deposit activity reports, into anti-money-laundering procedures.

Verify Your Bank Has No Correspondent Accounts
According to section 313 of the Act, banks are not allowed to maintain correspondent accounts with shell banks that lack a physical presence in any country. This provision exempts shell banks affiliated with a financial institution that has a physical presence in the U.S. or a foreign country, provided the shell bank is subject to supervision by a banking authority or regulated affiliate. The correspondent account regulations will have minimal impact on the nation’s community banks. In an alternative to tackling the responsibilities of maintaining correspondent accounts, many community banks connect their correspondent accounts to larger U.S. financial institutions. It is the larger institutions that maintain the desire to transact with foreign entities, while the basic goal of a community bank is to provide friendly, efficient service to the local community—not the global community.

Maintain Required Due Diligence
The Act has given U.S. financial institutions an obligation to increase their vigilance regarding correspondent accounts. The new due-diligence elements of section 312, which were issued as an interim final rule effective July 23, 2002, require U.S. financial institutions to establish policies, procedures, and controls to detect and report any known or suspected money laundering on behalf of a non-U.S. individual. In addition to this general requirement, the Act creates a minimum checklist of due diligence to perform in certain correspondent accounts. This checklist is applicable to those correspondent accounts being maintained for a foreign bank operating under an offshore license or a license granted by a jurisdic-
tion designated as being of concern for money laundering. Because most community banks do not maintain correspondent accounts, this section of the Act becomes less important. However, community banks should address this section in their BSA/anti-money-laundering policy. Banks have two alternatives when addressing this issue:

1. Simply state that they currently do not have any correspondent accounts and do not intend to acquire any in the future.

2. Include the minimum procedures set forth in the Act.

---

**Checklist 4**

**Minimum Due-Diligence Requirements**

☐ Does the bank ascertain the identity of all owners of the foreign bank?

☐ Does the bank maintain current information on lines of business and sources of wealth of the foreign bank?

☐ Does the bank determine the source of funds?

☐ Is the owner a senior foreign political figure?

☐ If so, does the bank report any known or suspected violation of law?

---

**Share Information with Your Neighbors**

Many community banks may be alarmed by the suggestion to share information with their neighbors. Some regulations passed a few years back made it more difficult for banks to share customer information with unaffiliated entities. However, section 314 of the Act now encourages banks to share information with financial institutions and federal law enforcement agencies. The regulators believe the information-sharing provisions will be a critical tool in the fight against terrorism.

Section 314(a) provides law enforcement agencies with a mechanism to provide banks with the names of specific suspects. The bank is required to report back to the Financial Crimes Enforcement Network (FinCEN) any matches based on such suspect information. In an attempt to minimize this research burden on banks, the regulators have limited the searches to accounts maintained during the preceding 12 months and transactions and funds transfers conducted during the preceding six months. In response to the authority granted by section 314(a) of the Act, FinCEN began soliciting from U.S. financial institutions information on suspected money laundering and on individuals and entities possibly tied to terrorist activities, a move that created several operational problems. As a result, on November 26, 2002, the Department of the Treasury issued a moratorium on section 314(a). The moratorium will remain in effect until all logistical problems are resolved.

In addition to the moratorium of section 314(a), the regulators announced the discontinuation of the Control List and unveiled a new process for managing information requests from law enforcement agencies. The Control List, created in response to the September 11 attacks, allowed FBI officials to communicate with financial institutions. The list was constructed by many law enforcement agencies and identified individuals and entities believed to be associated with terrorist activities. The regulating agencies have indicated that instead of the Control List, the FBI will use the section 314(a) information request process to communicate with financial institutions about persons suspected of engaging in terrorist activities. To ensure success in information distribution, the regulatory agencies have asked all financial institutions to verify that FinCEN has the most complete and up-to-date contact information for their banks. If your bank has not received any FinCEN requests since November 4, 2002, you should contact your primary regulator and ask to be added to FinCEN’s contact list. Moreover, it is imperative that your bank designates specific staff members to handle 314(a) requests. Because this process is intended to remain confidential, you should limit the number of employees allowed to manage and process the requests.

Section 314 also gives financial institutions the authority to share information with their neighboring financial institutions. The regulators believed that some method of notice should be imposed for financial institutions to indicate their intent to share information. In response to comments received about the proposed rule, the final rule has been changed to require that banks provide FinCEN only with notice of their intent to share information. Further, this notice may be sent before the bank decides whether
it is going to share information with its neighbors. This is contrary to the written certification process that had been proposed earlier. The final rule does retain that a new notice be given to FinCEN every year if the bank intends to continue sharing information. Additionally, prior to sharing this information, banks should take reasonable steps to verify that the institution with which it is sharing information has provided notice to FinCEN.

Checklist 5  
**Information-Sharing Requirements**

- Upon request from law enforcement agencies, does the bank have processes in place to research and report back to FinCEN any information regarding the suspect?
- Has the bank formed its intent to share information with its neighbor?
- If so, has the bank given notice to FinCEN of its intent?
- Has the bank verified that the neighboring institution has provided notice to FinCEN?

Create a Foundation for Customer Identification Procedures

Many bankers remember the proposed Know-Your-Customer rules of the mid-1990s. The regulators proposed the KYC rules, only to pull back after a significant uproar concerning privacy. Interestingly, the majority of comments came from the public, not the banks. Today, however, the USA PATRIOT Act has implemented a similar KYC rule known as the Customer Identification Procedures.

Indeed, the days of opening a bank account with a driver’s license and a smile are history. The proposed rules indicate a set of “minimum standards” that satisfy these regulations, but the rules remain only proposed, though they were originally scheduled to be finalized on October 25, 2002. The Department of the Treasury announced that it will publish final regulations implementing section 326 of the Act within six months of that date.

When finally issued, these new rules, already given the acronym “CIP,” promise to cause the biggest burden to financial institutions. They will require new procedures, systems changes, and a significant effort to increase employee knowledge of customers. While you should take a wait-and-see approach before implementing the new rules, all banks will want to watch closely when the final rules are published.

A Noble Act

Bank compliance officers are busy! Just after completing implementation of the Gramm-Leach-Bliley Privacy Regulation, Congress has brought us another implementation nightmare. Owing to the strong compliance management function, banks must realize that implementation of this new law will need to be a bank-wide effort. On the other hand, significant portions of the new law affecting banks are merely extensions of current programs. Therefore, the learning curve should be fairly shallow. Finally, while compliance officers are indeed busy, they clearly see the urgency and importance of stopping the cash flow to terrorism organizations.

Events tied to the USA PATRIOT Act are quickly and continuously unfolding. This article went to press at the beginning of January 2003.

Contact Schriner and Martinson by e-mail at rsm.compliance@rsmi.com or visit the Web site at www.rsmmcgladrey.com