From the Examiner's Desk...

This regular feature focuses on developments that affect the bank examination function. We welcome ideas for future columns, and readers can e-mail suggestions to ***SupervisoryJournal@fdic.gov.***

More than two-and-a-half years have passed since President Bush signed the USA PATRIOT Act into law in October 2001.[1] The USA PATRIOT Act strengthened measures to prevent, detect, and prosecute terrorism and international money laundering activities. The banking agencies have issued new anti–money laundering (AML) regulations during the past year. This article surveys some of the issues these regulations have raised for bankers and examiners.

Information Sharing and Customer Identification Programs Are Key Components of Bank Compliance

Two sections of the USA PATRIOT Act have generated the greatest volume of inquiries from banks and industry trade groups—Section 314 (Information Sharing) and Section 326 (Customer Identification Program).[2] As part of its compliance with Section 314, the Financial Crimes Enforcement Network (FinCEN) fields law enforcement requests for searches of names believed to be involved in money laundering or terrorist financing activity. Twice a month, FinCEN forwards a list of these names to all insured institutions and asks them to try to match these names with certain records covering a particular period of time.

During the past 15 months, FinCEN has consulted with financial institution regulatory agencies, the banking industry, trade groups, and federal law enforcement personnel and is now prioritizing the names subject to Section 314(a) requests. Law enforcement has benefited significantly from this program (see inset box). Many of the banks' positive responses have resulted in the identification of new criminal accounts and transactions and have helped law enforcement allocate scarce resources. Examples of initial successes include identification of the following: a Hawala operation involving a blocked country, arms and drug traffickers, alien smuggling resulting in fatalities, an international criminal network involved in identity theft and wire fraud, and a nationwide investment fraud scheme.[3] Although the government is in the early stages of prosecuting these cases, the Information Sharing program has contributed to law enforcement success in these areas.

Section 326 of the USA PATRIOT Act modifies the Bank Secrecy Act (BSA) and requires banks to develop a Customer Identification Program (CIP) that verifies customer identity, compares names with terrorist lists, and maintains appropriate recordkeeping. The CIP final rule took effect on June 8, 2003; however, financial institutions had until October 1, 2003, to implement a customer identification program. The design and implementation

Initial Results from the Information Sharing System

The Section 314(a) system has processed 188 law enforcement requests submitted from February 18, 2003, through November 25, 2003. Of these cases, 124 were related to money laundering and 64 cases were related to terrorism or terrorist financing. There were 1,256 subjects of interest in these investigations. Of these, financial institutions responded with 8,880 matches, resulting in the discovery or issuance of the following:

795	New accounts identified
35	New transactions
407	Grand jury subpoenas
11	Search warrants
29	Administrative subpoenas/summons
3	Indictments

[1]The complete title of this legislation is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001." Sections 314 and 326 (included in Title III of the Act) are not subject to the sunset provisions that apply to other subtitles of the USA PATRIOT Act. Section 324 of the USA PATRIOT Act requires the Secretary of the Treasury, along with the Attorney General, the banking agencies, the NCUA, and the SEC to evaluate the operations of the provisions of Title III of the Act and make recommendations to Congress as to any legislative action, if deemed necessary or advisable.

[2] The implementing rules for Section 314 of the USA PATRIOT Act are the Department of the Treasury's Financial Recordkeeping and Reporting Regulations, Sections 103.100 and 103.110. The implementing rules for Section 326 of the Act are the Department of the Treasury's Financial Recordkeeping and Reporting Regulations, Section 103.121 and the FDIC Rules and Regulations, Section 326.8(b)(2).

[3]Hawala (also known as hundi) is a money transfer system without formal recordkeeping procedures that is used primarily in the Middle East, Africa, and Asia.

of a CIP vary from bank to bank. Small, community-based banks tend to know virtually all their customers; however, these institutions must document their programs in writing. On the other hand, larger banks have a greater client base and must implement tighter controls to verify customers' identities. Banks must formally consider what risks they will accept. For example, what documents will they accept as identification? When developing their CIP, bankers may raise questions about how thoroughly some foreign governments check the identities of individuals requesting foreign identification documents. In these cases, bank management must determine which foreign identification forms are acceptable.

Bankers also are keenly interested in CIP requirements for trust accounts, an evolving compliance area. Key issues that must be addressed include identifying the customer, trustee, and source of funds, as well as determining how the bank should verify identities on trust accounts. These issues have been discussed on an interagency basis, and guidance is expected to be issued in the near term. Given the newness of the CIP requirements, examiners should be aware that many bankers will need additional training and guidance.

Changes in the BSA Affecting Nonbank Entities

Provisions of the USA PATRIOT Act require all financial institutions, including money service businesses (MSBs) such as currency exchanges and money transmitters, to comply with the BSA and anti–money laundering requirements. All MSBs, as defined in the USA PATRIOT Act, were required to register with FinCEN by December 1, 2003. These businesses are licensed by the state but are examined for compliance by the Internal Revenue Service (IRS). The IRS is responsible for more than 160,000 MSBs and approximately 600 casinos or other gaming organizations in some 30 states, territories, and tribal lands. The CIP requires that MSBs perform due diligence on MSB customers just as the CIP requires banks to perform due diligence on bank customers. In addition, if a bank has an MSB customer, bank management must understand the MSB's business operations and its normal volume of cash transactions.[4]

Supervisory Strategies Differ among Banks

Supervisory strategies depend greatly on the nature of a specific bank's activities. For example, many community banks have very few foreign correspondent or payable-through accounts. For institutions with the potential for higher-risk transactions and activities, an examiner would be expected to expand the examination procedures appropriately. Examples include the following: reviewing cash transactions by sub-account holders, reviewing the audit of the foreign bank's operations, evaluating the institution's process for identifying foreign correspondent account holders, and determining the adequacy of the account approval process if the institution has an international correspondent relationship with a bank in a bank secrecy or money laundering haven.[5]

[4]The CIP is a "gatekeeper rule" in that it relates to the responsibility of financial institutions to know with whom they are doing business. As a means of reporting suspicious activities, the FDIC and other agencies encourage banks to perform due diligence and account monitoring for high-risk customers, such as MSBs.

[5]FDIC BSA guidelines have expanded procedures that identify steps to be taken when a financial institution is involved in activities that have a greater risk potential. The guidance was released publicly on October 17, 2003, and can be found at www.fdic.gov/news/news/financial/2003/fil0379.html.

From the Examiner's Desk...

continued from pg. 33

Cooperation among Federal Bank Regulatory Agencies Is Critical

To strengthen the enforcement provisions of the USA PATRIOT Act, representatives from the Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board, Office of the Comptroller of the Currency, and Office of Thrift Supervision meet monthly to share information and best practices. Bank regulators also are working with federal law enforcement organizations (see inset box). This high level of commitment to national and global working groups that deal with USA PATRIOT Act issues and initiatives is notable.

Bankers and Regulators Work Together to Ensure Compliance

Compliance with provisions of the USA PATRIOT Act has received a great deal of attention during banker outreach meetings. A key issue raised by bankers is the lack of prompt feedback related to the filing of Currency Transaction Reports (CTRs). Approximately 12 million CTRs are filed annually, and, although it is not evident in all instances, federal and local law enforcement officials report that the data are extremely useful. However, understanding the need for CTR feedback, FinCEN, in consultation with the bank regulatory agencies, is evaluating options for

Interagency Groups

National BSA Advisory Group

- Meets twice a year
- Addresses anti–money laundering issues and initiatives
- Includes representatives from the FDIC, Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS), Conference of State Bank Supervisors (CSBS), bank trade groups, some large banks, the gaming industry, auto dealers associations, and the U.S. Securities and Exchange Commission (SEC)

Federal Bank Fraud Working Group

- Meets monthly
- Addresses current and emerging fraud issues
- Includes representatives from the Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS), U.S. Department of Justice, FDIC, Federal Reserve, National Credit Union Administration (NCUA), FinCEN, OCC, OTS, U.S. Postal Inspection Service, Bureau of Public Debt, and the U.S. Secret Service

Financial Systems Assessment Team (FSAT)

- Meets biweekly
- Works with countries that may be vulnerable to money laundering or terrorist financing. FSAT works with the judicial system, law enforcement personnel, and financial regulators in these countries to identify any potential problem areas, and provides training and technical assistance
- Sponsored by the U.S. State Department and includes representatives from FinCEN, U.S. Customs and Border Protection, OCC, Federal Reserve, FDIC, FBI, and other representatives from the Treasury and State Departments

providing input to the industry. FinCEN provides feedback on Suspicious Activity Reports (SARs) through SAR Activity Reviews (see links to recent reviews in the inset box). The SAR Activity Reviews are products of close collaboration among financial institutions, federal law enforcement officials, and federal regulatory agencies. The SAR Activity Reviews provide meaningful information about the preparation, use, and value of SARs filed by financial institutions.

As bankers implement and refine compliance programs, they are asking for guidance about what works and what doesn't work. They are concerned about relationships with foreign accounts, particularly those in the Caribbean. Guidance on these and other issues related to the USA PATRIOT Act exists in the form of Financial Institution Letters (FILs) and Frequently Asked Questions (FAQs) available on the FDIC's external website, www.fdic.gov. The FDIC has a website that is devoted specifically to issues related to BSA compliance and anti–money laundering activities (www.fdic.gov/regulations/examinations/bsa/). Overall, bankers are doing a good job of complying with provisions of the USA PATRIOT Act. However, bankers should remain vigilant, as they serve a vital role in the fight against money laundering and terrorist financing.

Key Issues for Examiners

Compliance with provisions of the USA PATRIOT Act is of significant concern to examiners as well as bankers. Examiners must ensure that the scope of review is appropriate. Examiners need to understand the risk attributes of the specific bank and should also review workpapers, CTR filings, and SAR activity since the last examination to determine the appropriate level of exam resources. As bankers must understand their frontline role, examiners must be knowledgeable about BSA and AML compliance requirements and be prepared to communicate and explain these requirements to bankers.

Because of its importance to national security, BSA and AML will continue to receive significant attention. Expectations are that more effective use of exemptions from CTR filings will help ensure that valuable resources are not diverted from investigations of threats and actual crimes. As new money laundering techniques are identified by law enforcement personnel, compliance and enforcement procedures will continue to change. For example, FinCEN recently released information about how jewels and precious metals are being used to launder money and support terrorist financing.[6]

Conclusion

Overall, the new BSA requirements have broadened the banking industry and regulatory approach to include measures designed to detect terrorist funding, an unfamiliar concept to most before September 11, 2001. However, failure to comply carries with it costs, such as enforcement actions, including civil money penalties, heightened reputation risk, and the significant social costs associated with money laundering or terrorist financing activities. Working together, examiners and bankers can successfully navigate this new chapter in bank compliance.

James J. Willemsen
Supervisory Examiner

Lisa D. Arquette, Chief, Special Activities Section, contributed significantly to the writing of this article.

Links to Recent FinCEN SAR Activity Reviews

SAR Activity Review Issue 6 (November 2003)
http://www.fincen.gov/sarreviewissue6.pdf

SAR Activity Review Issue 5 (February 2003)
http://www.fincen.gov/sarreviewissue5.pdf

[6] "FinCEN Urges Cooperation Against Use of Diamond and Precious Metals Trade to Support Terrorist Financing," March 29, 2004. http://www.fincen.gov/dubaipressstmnt.pdf and Remarks by FinCEN Director William Fox before the World Diamond Council, March 30, 2004, Dubai, United Arab Emirates. http://www.fincen.gov/dubaiconferenceaddress.pdf.