

The Evolution of



Anti-Money Laundering Compliance

by Carol M. Beaumier
and Sujal Shah

The enactment of the USA PATRIOT Act on October 26, 2001, was a direct response by the U.S. government to the terrorist activities of September 11, 2001. The Act's primary purpose is to strengthen the ability of the United States to prevent, detect, and prosecute international money laundering and terrorist financing. Despite its far-reaching scope and complexity, it was signed into law only six weeks after the terrorist attacks — an indication of the U.S. government's sense of urgency.

Title III of the act, the International Money Laundering Abatement and Terrorist Financing Act of 2001, extended anti-money laundering (AML) program requirements that previously had applied only to banks. The new AML standards apply to a broad group of financial institutions.¹ By introducing additional requirements such as enhanced due diligence (EDD) for correspondent and private banking accounts and a customer information program (CIP), the act raises the bar significantly for AML compliance.

As we pass the second anniversary of the passage of the act, its full impact on financial institutions and other stakeholders is still unclear. Implementing

It has been two years since the passage of the USA PATRIOT Act, which was enacted to thwart the efforts of terrorists zealously fixated on manipulating the financial system in the United States to fund their violent attacks. Since the act's passage, compliance officers have been mired in efforts to comply with the new rules and regulations on time, and to also keep up with changes and problem spots.

This feature examines the evolution of anti-money laundering compliance and what it means to those professionals charged with its implementation.

regulations continue to be promulgated amid occasional controversy, as was the case with CIP rules required by Section 326. These rules were first proposed in July 2002; issued in final form in May 2003; and then, in an unusual move, subjected to a "notice of inquiry" in July 2003 to seek additional comments about retaining photocopies of identification and reliance on certain forms of government-issued identification. However, after reviewing more than 34,000 comments, the Treasury Department determined that no changes were justified. October 1, 2003 remained the compliance date, but agencies had publicly indicated that banks would not be penalized for incomplete customer identification programs if they had made progress in most areas. To exam-

ine the Treasury's fact sheet on the decision to leave CIP rules alone, please visit: www.ustreas.gov/press/releases/reports/js7432.doc.

For some types of financial institutions, basic requirements — the Section 352 rules pertaining to the development and maintenance of an AML program — remain in proposed form or have yet to be addressed at all by the Treasury Department. Even the Section 352 rules issued for banks and savings associations in April 2002 are interim final rules, suggesting they could be subject to further amendment. The rule-making process highlights the complexities involved in adapting "one-size-fits-all" legislation to the diverse businesses of a broad range of financial

The rulemaking process highlights the complexities involved in adapting “one-size-fits-all” legislation to the diverse businesses of a broad range of financial intuitions. Not surprisingly, financial institutions continue to struggle to apply the requirements across numerous products and service offerings.

intuitions. Not surprisingly, financial institutions continue to struggle to apply the requirements across numerous products and service offerings.

Additionally, the industry is still waiting to see how the Treasury Department will use the broad authority provided to it under the act. For example, the special measures authority granted by Section 311 permits the Treasury Department to impose additional restrictions or outright prohibitions on a U.S. financial institution's ability to conduct business with specific jurisdictions or financial institutions, or to conduct particular types of transactions. Thus far, the Treasury Department has used this authority sparingly, most recently to issue a proposed rule that would bar domestic financial institutions from conducting business with financial institutions in Nauru. Similarly, the act affords the Treasury Department the right to issue regulations governing the use of concentration accounts, but there has been no action on this issue.

On another front, one section of the act may have gone unnoticed by the industry until recently. Some bankers were caught off-guard by the Justice Department's seizure, under authority of Section 319 of the act, of reportedly more than 15 correspondent accounts maintained in the United States that were owned by foreign banks whose customers were linked to fraud and money laundering investigations.² Under its Section 319 authority, the Justice De-

partment is not required to trace the funds deposited in the U.S. correspondent account to the proceeds of crime deposited in the foreign bank, nor does the U.S. bank (including a branch or agency of a foreign bank operating in the United States) generally have any legal standing to challenge the seizure. While the Justice Department continues to signal that it will use its seizure powers carefully and deliberately, this authority raises protests of extra-territorial application of U.S. law and concerns over potential litigation pitting a U.S. bank against its foreign correspondent and its customers.

Global initiatives

Internationally, we continue to see foreign governments strengthening their AML programs and multinational bodies issuing additional guidance. In June 2003, the Financial Action Task Force (FATF), which first published its “Forty Recommendations” setting minimum standards for money laundering prevention and detection in 1990, updated its guidance. The major changes essentially bring the FATF recommendations in line with existing U.S. requirements and include the prohibition of shell banks; the extension of the applicability of AML procedures to designated nonfinancial businesses and professions; the extension of AML requirements to cover terrorist financing; and enhanced measures for higher-risk customers and transactions, including correspondent banking and politically exposed persons.

In June 2003, the Basel Committee on Bank Supervision, the International Association of Insurance Supervisors, and the International Organization of Securities Commissions issued a joint document summarizing their initiatives for combating money laundering and terrorist financing within the banking, insurance, and securities sectors, respectively. The document highlights both the importance of group-wide risk management of money laundering risk by financial conglomerates and the need to tailor customer due diligence requirements to specific industry sectors.

Industry efforts

The private sector also continues to set standards and shape expectations for AML programs. In November 2002, for example, the Wolfsberg Group of International Financial Institutions³ published its Principles for Correspondent Banking, which, together with the New York Clearing House's “best practice” guidelines on correspondent banking, has shaped many AML correspondent bank compliance programs. Additionally, trade associations and self-regulatory groups, including but not limited to the American Bankers Association, the Securities Industry Association, the Managed Funds Association, and the National Association of Securities Dealers, continue to issue guidance to the financial services industry.

Regulatory environment

While the rules and expectations continue to develop, much of the regulatory focus — if measured by enforcement actions — continues to be on the banking industry. Interestingly, in 2003 many of the targets of these enforcement actions have been community banks, which historically may not have considered money laundering a significant risk.

Among the common themes identified in the enforcement actions are inadequate reporting and recordkeeping, deficient know your customer (KYC) and monitoring procedures, inadequate training programs, and lack of independent testing of the AML program.

Coping with the major challenges

The basic requirements of an AML program sound simple:

- Develop policies, procedures, and internal controls.
- Designate a compliance officer.
- Conduct training.
- Perform periodic independent testing of the program.

However, many financial institutions are coming to realize how difficult it is to develop and maintain an effective AML program. One of the first hurdles AML compliance officers may face, particularly from a budgetary standpoint, is convincing boards of directors, senior management, and others of the enormity of the undertaking. Indeed, at times the AML compliance officer may not appreciate what is expected and succumbs to the temptation to put his or her organization's name on the model AML policy issued by a trade association with little attention to whether, on a day-to-day basis, the organization is actually doing what the policy suggests.

Another common problem is that financial institutions respond to the Act and other regulatory requirements on a piecemeal basis without having a vision of what the complete AML program will be — e.g., they develop KYC/EDD standards without regard to what information they need for risk assessments or moni-

toring purposes. In these circumstances, institutions often find themselves needing to revise parts of their AML program so that all of the initiatives align.

In addition to the foregoing, certain AML program elements are being identified as particularly challenging, both for banks upgrading their AML programs to address new USA PATRIOT Act requirements and regulatory expectations and for other financial services companies developing their initial programs. These include developing a risk assessment methodology, striking the right balance between traditional KYC requirements and EDD, and transaction monitoring.

Customer risk assessments

Understanding the money laundering risk of the products and services offered by a financial institution and the institution's customer base is key to designing an effective AML program. The results of the risk assessment — particularly a determination that a particular customer type poses a higher money laundering risk — should drive the level of due diligence (KYC/EDD) conducted at the time the customer relationship is established, the extent of monitoring of the customer's transactions, and the frequency and scope of updating information about the customer.

A money laundering risk assessment methodology should incorporate, as applicable, the following factors:

- type of product or service the customer is requesting or has
- nature of the customer's business
- geographic considerations such as the residency or principal place of business of the customer

- financial institution's prior experience and knowledge of the customer and his or her transactions
- expected pattern of activity in the account
- expected origination and destination of funds
- method of account opening (e.g., face-to-face, mail, Internet, etc.)

In certain instances such as correspondent banking, the risk assessment methodology may need to be expanded to consider the type and nature of the customers of a financial institution's customer.

Attempts to "risk rate" a customer base sometimes fail because those conducting the risk assessment, especially when they are the individuals responsible for generating the customer relationship, do not understand the objective of the exercise and believe that assigning a "high" risk rating will automatically result in termination of the customer relationship. Additionally, as noted above, risk assessment methodologies may fall short because they do not adequately take into consideration all of the variables that may be important for monitoring purposes. As a general rule, financial institutions should be prepared to improve and refine their risk assessment methodologies over time as they gain more experience through monitoring their customer base. However, they should consider as many variables as possible at the onset, clearly communicate the risk assessment objective, conduct training with examples of how the risk assessment methodology should be applied, and ensure consistent quality control by the AML compliance department. All of these steps will contribute to a better outcome. ►

Balancing a CIP with enhanced due diligence procedures

The final CIP rules issued in May 2003 outline the minimum customer identification requirements. Beyond these requirements, the rules require each institution's CIP to be risk-based. That means that the extent of information requested need not be the same for every customer. For example, a customer who maintains a retail savings account does not need to provide as much information as the local merchant who maintains a business checking account and makes frequent cash deposits. It also means that the institution should perform EDD and obtain additional information for a customer deemed to pose a higher money laundering risk.

EDD procedures, by their name, are expected to be additive to KYC procedures. They may include more in-depth questions about the customer's financial resources, additional steps to validate information provided by the customer, utilization of the Internet or other means to conduct additional research about the customer, or even hiring an investigative firm.

As financial institutions implement EDD procedures, we see some instances where, in fact, they simply repackage their KYC procedures without substantive change, or where they do expand their procedures but perform EDD for all customers, resulting in an inefficient and burdensome process. Both of these approaches undermine the intent of EDD.

Another pervasive issue is that although account officers may know their customers well and can verbally demonstrate that knowledge, their familiarity is

often not documented properly in customer files. Apart from the fact that turnover among account officers can result in a loss of critical information, this issue suggests these institutions will be unable to demonstrate knowledge of their customers to regulators. In the current regulatory environment, if isn't documented, it doesn't count. Ensure properly documented client files via adequate training of account officers and an ongoing quality control program.

Transaction monitoring

Among the common deficiencies identified in regulatory examinations, and likely the most challenging aspect of maintaining an effective money laundering compliance program, are transaction monitoring procedures. Even though banks were required to monitor transactions for potentially suspicious activity before the enactment of the USA PATRIOT Act, many are only now beginning to realize the full implications of monitoring and the corresponding strain on resources.

Initially, most institutions decide to monitor transactions manually. For smaller, less-complex organizations, manual monitoring is still a viable alternative. However, as institutions grow in size and offer a broader range of products and services, it becomes increasingly unrealistic to rely on manual monitoring. With the enactment of the USA PATRIOT Act and the increasing availability of AML monitoring software, many financial institutions are now selecting automated transaction monitoring systems to reduce (but not eliminate) the manual effort required. Many international institutions are choosing to select AML software on a global basis to enhance efficiency and consistency throughout their global operations.

Although there are no regulations requiring U.S. financial institutions to use automated software, regulators are increasingly encouraging, and in some cases pressuring, the adoption of such software. In June 2003, Switzerland set a precedent by becoming the first country to issue rules requiring banks and securities houses, with the exception of smaller institutions of an as-yet-unspecified size, to use automated AML systems. Whether the United States will follow Switzerland's lead on this issue is uncertain; however, examiners likely will continue to exert moral suasion to convince financial institutions of the value of automated systems.

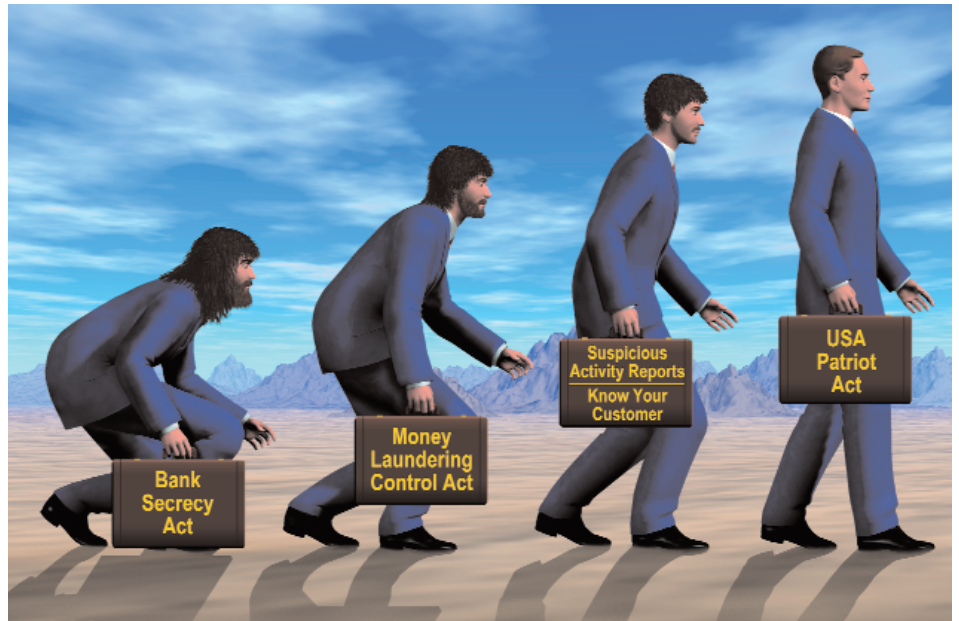
AML software runs the gamut from simple rules-based systems to sophisticated artificial intelligence systems. The decision to purchase AML software must be predicated on a number of considerations, including system requirements and functionalities, capacity, ease of use, the vendor's reputation and sustainability, and cost.⁴

While AML monitoring software can significantly enhance a financial institution's ability to monitor transactions for suspicious activity, it is a tool, not a solution. Many institutions have been criticized during regulatory examinations for overreliance on automated monitoring software without fully understanding how the software is designed and what information it does and does not capture. During the implementation of automated software, a financial institution needs to dedicate sufficient resources to ensure the software is customized to its business and customer profile. Some institutions have incorrectly assumed that vendor implementation of the software will satisfy the financial institution's re-

sponsibility to monitor transactions and that no further effort by the institution will be required. They are forgetting, of course, that qualified individuals will still need to interpret information generated by the system to decide whether or not a suspicious activity report (SAR) should be filed. Also, they often do not realize that, upon initially converting to an automated system, a financial institution is likely to face a significantly larger number of unusual transactions to investigate compared to the manual monitoring process.

Additionally, even the most sophisticated monitoring software cannot replace one element of manual monitoring: Employees who deal directly with customers or process customer transactions are in the best position to know customers and whether transactions constitute normal activity. Financial institutions need to ensure that their employees receive adequate training to identify potentially suspicious transactions, and that all employees understand the importance of their role in transaction monitoring.

While transaction monitoring should be risk-based, the focus should not be on high-risk transactions alone, particularly as money launderers are becoming increasingly sophisticated and will seek ways to target an institution by using transactions that are least likely to be monitored. All transactions require a degree of monitoring and the exclusion of certain transactions from monitoring presents a risk to the financial institution. This case is well illustrated by what we have come to learn about the financing of the September 11 terrorist attacks. While some of the terrorists' transactions did involve in-



ternational wire transfers to and from jurisdictions that would be viewed as higher risk, many were small domestic transactions that would have been below the monitoring thresholds of most institutions.

Looking ahead to the next generation of AML programs

Where does AML compliance go from here? Answering that question first requires speculating about how AML regulation and supervision will evolve. On the global front, it is reasonable to expect that countries will continue to move, or be prompted by the international community to move, toward a common AML framework, reducing the opportunity for money launderers or terrorists to arbitrage tax regimes. It is also likely that secrecy laws, which have frustrated AML efforts, will continue to erode. Domestically, we are likely to see enforcement actions extend beyond the banking industry into other sectors of the financial services industry, as regulators in other sectors

become more comfortable with the requirements and as the “grace period” of the initial AML program implementation phase expires.

For obvious reasons, industry participants will continue to look for ways to pool resources and share information. This may take the form of industry alliances, such as the one formed by Goldman Sachs and other large financial institutions last year to develop a public records database,⁵ or private sector initiatives to support centralized KYC repositories. These efforts, however, are likely to continue to be subject to privacy challenges. In the United States, we may also see increased participation by financial institutions in information sharing under Section 319(b) of the USA PATRIOT Act.

AML compliance programs will increasingly rely on technology as the number of vendors and choices continues to increase and perhaps makes technology a more affordable alternative for a larger group of institutions. Additionally, finan-

cial services companies will continue to add sophistication to their AML program methodologies by, among other things, refining and enhancing risk assessment methodologies.

The USA PATRIOT Act contains a sunset stipulation under which all of its provisions may terminate after September 30, 2004, if Congress determines they are no longer necessary. With our final look into the future, we predict that counting on Congress to roll back the Act's provisions next year would be a very bad bet. ❖

Have a question or comment?

Use the postage-paid reply card provided in this issue or leave a message at (202) 663-5075.

about the authors

Carol Beaumier is a managing director with Protiviti and leads the firm's financial services and regulatory risk consulting practices. A former bank regulator, Ms. Beaumier has extensive experience with anti-money laundering and OFAC compliance programs. She can be reached at (212) 603-8337 or carol.beaumier@protiviti.com.

Sujal Shah is a senior manager with Protiviti, specializing in the financial services practice. She has in-depth knowledge of anti-money laundering and OFAC regulations. Reach her at (212) 603.8337 or sujal.shah@protiviti.com.

1. As defined in the USA PATRIOT Act, a financial institution is, but is not limited to, the following: a bank; a broker-dealer; an insurance company; a money service business; a loan or finance company; a casino; a pawnbroker; a travel agency; a business engaged in the automobile, airplane or boat sales; and a dealer in precious metals, stones or jewels.

2. "U.S. Cautiously Begins to Seize Millions in Foreign Banks," *New York Times*, May 29, 2003.

3. The Wolfsberg Group consists of the following leading international banks: ABN Amro N.V., Banco San-

tander Central Hispano, S.A., Bank of Tokyo-Mitsubishi Ltd., Barclays Bank, Citigroup, Credit Suisse Group, Deutsche Bank AG, Goldman Sachs, HSBC, J.P. Morgan Chase, Societe Generale, and UBS AG.

4. "Effective Anti-Money Laundering Monitoring: Issues and Challenges," Carol M. Beaumier and Carl J. Hatfield, *Bank Accounting & Finance*, Volume 16, Number 2, February 2003.

5. "Goldman, Other Firms Joining in Launder Database Venture," *American Banker*, June 3, 2002.