



Challenges In the Wake of the USA PATRIOT Act

by Steven Lindseth and
Theodore Frank

While most agree that the USA PATRIOT Act, with its goal of reducing money laundering and terrorist activities, is in the best interests of the industry as well as society as a whole, how good are the act's regulations if they cannot be implemented effectively?

Many banks are responding to the USA PATRIOT Act like any other compliance initiative. Banks are implementing additional chains of command, new sets of policies and procedures, and ad hoc technology solutions. But this is like fighting a fire with a bucket brigade — the fire might eventually be extinguished, but nothing is put into place to prevent the next fire. What's needed? A consistent methodology that extends across the entire enterprise, ensuring that appropriate policies around suspicious financial transactions and other core requirements of the act are defined, communicated, and followed every day by the correct groups of people, both employees and partners. Notwithstanding the ability to monitor transaction systems, humans are still involved in the myriad standard operating procedures that will stem from

Managing compliance under multiple statutes and regulations is a major undertaking for banks — one that continues to grow more complex with the passing of each new regulation, such as Sarbanes-Oxley and, most significantly, the USA PATRIOT Act of 2001. Navigating in the sometimes-turbulent waters of these new rules requires greater focus and understanding throughout the many departments inside banks. Having the right technology and a strategy is just the beginning.

the act, and judgment will still play a role in effective compliance with it.

Most banks have developed effective systems to ensure they meet their numerous compliance obligations, but few have developed strategic, integrated solutions to ensure they stay in compliance after the compliance protocols have been mapped out, while providing a global compliance dashboard required at the senior management and board levels.

To efficiently comply with the USA PATRIOT Act and other regulations a bank must leverage technology to bridge the gap between strategy and execution.

To be successful, a financial institution not only must rely on its numerous transaction systems and the monitoring technology these systems employ, but also must tie these to a single, comprehensive solution that provides visibility into all compliance responsibilities and the people who drive them. This will ensure that data and people are connected within a defined framework.

Given these new regulations, effective compliance management can be achieved only by applying the same principles that have been successful in other business areas, such as CRM, ERP, or core transaction systems themselves. The problem is that the numer-

ous compliance policies will impact virtually every employee in different combinations, sometimes by business unit, geography, job function, etc., and those who are responsible for managing these policies may be doing so as an adjunct to their primary jobs. It is time for every financial institution to implement more comprehensive compliance technology to automate policy-driven processes and develop a consistent methodology focusing on this complex and ever-changing matrix of roles and responsibilities. Most institutions struggle to define and change/manage this matrix effectively, so policies and standard operating procedures can be made operational effectively.

Seven steps to effective compliance

The federal government and the U.S. Sentencing Commission established a consistent methodology for managing compliance. The seven-step framework comprehensively addresses the key issues of an effective governance and compliance program:

- policies
- high-level oversight
- proper delegation
- effective communication
- auditing and monitoring
- uniform enforcement
- continuous process improvement

The framework is an effective guideline to help manage the multitude of compliance initiatives, but few institutions' programs meet the seven steps. As a result, visibility and performance reporting efforts across various compliance initiatives are hindered.

Why the USA PATRIOT Act makes compliance more difficult

The USA PATRIOT Act has a number of intricacies that make compliance particularly challenging. As new requirements of the act go into effect, the challenges facing financial institutions increase. It is critical that banks leverage technology to

Federally Mandated Seven Steps of Compliance

The federal government, through the Office of Inspector General and the United States Sentencing Commission, has mandated seven steps every compliance program must take to be accepted as a means of meeting compliance obligations imposed by various federal statutes and regulations. Though these steps were originally enumerated to assist federal judges in assessing criminal penalties, they have since been applied to noncriminal, regulatory situations through the Office of Inspector General. The seven requirements for an effective compliance program are as follows:

1. Policies and procedures: Develop policies and procedures to institutionalize and encourage appropriate behavior.
2. High-level oversight: Create a role specifically responsible for compliance management and performance.
3. Decentralized administration and proper delegation: Designate appropriate accountabilities and exhibit due care in delegating discretionary administrative authority.
4. Establish communication channels: Provide effective communication among all levels of employees.
5. Audit, monitor, and reporting: Compliance efforts must be monitored and audited to ensure the programs are effective.
6. Uniform enforcement: Policies and procedures must be enforced and when exceptions are discovered, consistent corrective action must be applied.
7. Prevent further offenses: Use performance information to prevent further similar offenses after a violation has been detected. (For more government information, visit www.ussc.gov/2001guid/8a1_2.htm.)

successfully address these new requirements as they become effective, and also be leveraged to address other compliance requirements, all within a consistent and seamless environment.

Financial institutions and other businesses are responding to the requirements via a number of programs, including anti-money laundering programs, customer and employee identification programs, suspicious activity reporting programs, and bank secrecy programs. As more financial institutions become subject to suspicious activity reporting duties, there is increased risk that institutions will be prosecuted or penalized for not filing reports. So while most institutions are struggling to build effective customer identification programs, sound suspicious activity detection and reporting are proving to be the pillars of self-protection in the anti-money laundering field. The challenge is tying this data to a consistent response protocol that is managed by the appropriate people, while the appropriate people are changing jobs or roles within the organization.

Establishing policies and procedures to meet all the USA PATRIOT Act provisions is tough enough. Communicating, tracking, and managing all of the new rules, regulations, and risks associated with the act is an even bigger challenge, because it involves the entire institution — including human resources, accounting, security departments, the board of directors, and auditors.

So while most institutions are struggling to build effective customer identification programs, sound suspicious activity detection and reporting are provided to be the pillars of self-protection in the anti-money laundering field.

Solutions must be able to grow with the company, respond to the changing business environment, adapt to new regulations, manage ongoing compliance activities, and most importantly, improve visibility, transparency, and performance reporting across the organization.

Financial institutions must be prepared to facilitate the education of all their stakeholders about the Patriot Act, anti-money laundering laws and regulations, other applicable rules for investor identification, and suspicious activity reporting. It is the duty of every institution to create a system of checks and balances in which rules and requirements are made clear to every employee, questions can be asked, and potential violations can be both detected and reported in as close to real time as possible.

In short, a bank will not be able to respond to the USA PATRIOT Act's reporting or training requirements unless it implements an end-to-end solution that addresses each of the seven-steps of effective compliance. Doing so is the only way a bank can gain a complete view of customer activities and transactions while detecting danger zones in customer acceptance, managing suspicious activity, and automating essential investigations processes and guidelines.

Solutions for compliance

Clearly, the agencies and Congress are focused on having financial institutions improve policies and procedures, com-

pliance response, staff training, and due diligence. As a result, financial institutions can't simply update their programs to comply with the act — they must change the way they have historically approached their business systems. This will require a great deal of commitment at the top, along with investment in technology and people to design and implement an infrastructure to comply with the act.

The USA PATRIOT Act is forcing banks to employ a consistent approach using a more comprehensive framework. Solutions must be able to grow with the company, respond to the changing business environment, adapt to new regulations, manage ongoing compliance activities, and most importantly, improve visibility, transparency, and performance reporting across the organization.

To respond to these broad industry challenges, a financial institution must employ a solution with a highly secure environment that allows it to:

- document and manage all compliance responsibilities, policies, procedures, training, FAQs, processes, etc., in a single environment;
- define behavioral and procedural requirements for all employees and partners;
- monitor disparate systems and trigger investigation of potential exceptions, such as suspicious transactions; and

- gain visibility across the entire enterprise so management (and regulators) can see whether and how compliance management is working, measuring the effectiveness of policies and procedures according to the seven steps defined by the federal government.

After the USA PATRIOT Act

Combined with other regulatory mandates and market drivers, such as the Sarbanes-Oxley Act, organizations subject to the USA PATRIOT Act have little choice but to build or buy more comprehensive, consistent, leverageable, and integrated compliance central nervous systems that can be extended worldwide to employees and business partners.

As a start, every financial institution should review the seven steps of effective compliance as defined by the federal government through the Office of Inspector General and the U.S. Sentencing Commission and determine how its own compliance management protocols compare to the list. If they fall short, it is time to consider implementing something more comprehensive.

Though the expense of creating a compliance system that really works can be significant, the risks and potential costs of compliance failure are too great to ignore. ❖

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

Steven Lindseth is the chairman of Axentis LLC and **Ted Frank** is the president and CEO of Axentis LLC, which provides governance and compliance software to large organizations. Both can be reached at (440) 519-2929. The company Web site is www.axentis.biz

| FRAUD PREVENTION



THINK OF US AS A FLAME-RESISTANT COATING.

From training to software,
we can help you protect your profits.



1.800.552.9410 www.bankerssystems.com

241484