Knowing Your Customer and Culture: An Integrated Approach to USA PATRIOT Act Compliance

By Vincent Manning, *Venture Financial Systems Group, LTD.*, Marc Spitzner, *Venture Financial Systems Group, LTD.*, Ralph C. Martin II, *Bingham McCutchen*, Donald J. Savery *Bingham McCutchen*

The financial markets are still sorting through the lengthy list of compliance measures created by the Sarbanes-Oxley legislation and other reforms being proposed by the SEC, NASDAQ, state attorneys general, institutional investors, and others. This preoccupation should not derail corporate efforts to comply with the mandates of the USA PATRIOT Act, an especially important measure that is applicable to companies defined as "financial institutions" by the Act. The Act has several purposes: to better detect and deter incidents of money laundering; prevent financing of terrorist activity; and more severely penalize those who launder money, by strengthening, broadening and clarifying federal money laundering laws. The Act aspires to meet these challenges by requiring financial institutions to exercise a more rigorous due diligence in the following undertakings:

- Identifying people who control assets,
- Determining the origination of funds coming into the U.S. financial system,
- Identifying the destination of funds funneled through the U. S. financial system, and
- Determining veiled or undisclosed purposes for financial transactions, especially so-called "suspicious" transactions.

Passage of the USA PATRIOT Act represented a strong and immediate response to a growing domestic and global threat. The wide-ranging provisions of the Act apply to a broad array of financial institutions, which (as defined in the Act) include banks, credit unions, broker/dealers, mutual funds, venture capital firms, and others. For many of these institutions, compliance with the Act's requirements presents one of the greatest operational challenges they have ever faced.

The fundamental risk that the Act seeks to address is based upon recognition that terrorists and their financial supporters seek to funnel money through western financial clearing houses. They utilize foreign accounts, false identities, shell companies, and disguised purposes to fulfill their terrorist missions. They also seek to smuggle cash, financial instruments, and other assets of value that can be traded for cash. Therefore, compliance with the Act contemplates that potential violations of the Act can occur across business lines, subsidiaries, and products. For a financial institution, becoming compliant requires an alignment of operational and technical lines of business on a level rarely seen.

Full compliance depends on cooperation among a variety of intra-organizational business areas, including compliance, legal, trading, information technology, systems, and back-office personnel. It demands buy-in at every level from senior management to entry-level customer-service representatives. The success or failure of a company's efforts to comply with the Act will depend on how successfully the company can integrate its risk management efforts across business and operational lines. Compliance requires skillful project management and resource integration in the implementation and maintenance of an integrated solution. In short, compliance with the Act needs to be integrated into the company's overall risk management protocol and mindset.

Most financial institutions have already implemented or are in the process of implementing business processes and systems to adhere to the new laws. However, implementation of a solution cannot be achieved simply by using "add-on" components such as plug-and-play technologies that are bought off-the-shelf. So far, many institutions have relied predominantly on technological solutions to assure themselves of compliance. Technology, without human judgment and forensic insight, is not enough to ensure compliance with this Act, which particularly requires financial institutions to "know their customer."

Compliance with the Act requires operational and technical solutions that many financial institutions do not have the capacity either to define or implement. Without a proper analysis of the legal requirements of the Act and an assessment of the impact of those requirements on the activities of a given institution, even identifying a starting point for compliance projects can be an enormous task. Given the potential for large penalties in the event of noncompliance, the stakes are high.

The Act requires financial institutions to establish minimum standards of compliance that include the following components:

- The development of internal policies, procedures and controls;
- The designation of a compliance officer;
- An ongoing employee training program;
- An independent audit function to test programs.

Full compliance requires leadership from senior management in the same fashion that other firm-wide visions for product improvement, business solutions, or other business imperatives of the firm are implemented. Anti-money-laundering (AML) leadership must be exercised by senior management through a consistent, firm-wide vision for implementing solutions. Project success is possible only if management first recognizes that compliance must shift from a departmental focus to a firm-wide effort. While the Act requires institutions to "know their customers," implementation mandates that companies "know their culture" as well. Aligning the proper project phases will go a long way toward achieving success on both fronts.

The roadmap to compliance can be divided into five distinct phases: *Assessment* of the firm's risk and capabilities; *design* of a solution; *implementation* of the solution; *training* of all personnel; and *continued monitoring* for operational and/or legal changes.

Assessment. Assessment of the current operational and legal landscape is of critical importance in determining an appropriate compliance solution. In the absence of regulations promulgated by the Treasury Department, financial institutions are left largely on their own to implement AML efforts. Even as various industry organizations such as the Investment Companies Institute (ICI) and National Investment Company Service Association (NICSA), continue to press for clarification of PATRIOT Act requirements, firms must move ahead with their compliance projects. Involvement of third-party consultants at the assessment stage can be key to ensuring full compliance with the law.

The assessment phase of the project should begin with an expert analysis of general industry risks, as well as risks specific to your particular firm. Financial institutions vary by size, lines of business, type of ownership, geographical location (national vs. multi-national), etc. A thorough and contemporary analysis of the firm's management and organizational structure and its scope of business is needed before a plan may be devised. To accomplish this, the firm must ensure that all affected departments and divisions are given an accountable role. It is critical to establish the presence of legal and operational experts at the center of the project. The core project team members must be representative of the company's key business and operational units and be lead by someone with enough power and stature to command cooperation during this effort.

The focus of the assessment then moves to analyzing the existing and untested capabilities of the organization in light of the legal and technical requirements. Firms must understand the law. The Act and AML regulations can be complex, and noncompliance can result not only in heavy fines, but also in the loss of a firm's hard-earned reputation. A comprehensive legal review of the firm's business processes needs to be completed to surface legal vulnerabilities in current procedures and data management. Once gaps are exposed, the firm can move to the design and implementation of the appropriate solutions.

Design. With assessments completed, the project moves into the design phase. At this point, the project team will understand the law and be aware of gaps in current procedures and systems that expose the firm to compliance violations. The solution must incorporate both technical and operational elements that many firms are not in a position to assess on their own. For instance, a thorough evaluation of available products should be carried out. A firm must determine if off-the-shelf or design-to-build products can reduce certain level(s) of risk, and if so, what exposures will remain after a product is adopted. If there is continued exposure, can procedures be created to cover the gaps? A firm also should examine the scalability of available systems and identify who will be responsible for upgrading those systems to account for new or enhanced regulations.

While the technical evaluation is underway, it is equally important to examine the impact of any new data requirements and/or operating procedures on workflows and client-interaction points. Implicit in the Act's objective is the requirement that institutions upgrade their ability to judge data *and* customers.

Implementation. Once a product is selected, the project moves into the integration and implementation phase. Again, technical and operational coordination is pivotal. Data and processes from across the organization must be coordinated and reconciled. This effort will require the integration of disparate systems and cross-departmental cooperation. Firms typically must launch new systems and add new data fields to

existing systems. These technical challenges pose additional operational challenges. New procedures will need to be designed and tested to ensure that the firm's compliance is uniform and that it can withstand multiple threats. The SEC has stated that it will review the quality of firms' AML programs, including the design and implementation of those programs, as it determines whether or not the programs are adequate for the firm's businesses. This, again, demonstrates that compliance requires more than a "one size fits all" solution.

Training. The implementation of new systems and procedures does not represent the final phase of a solid AML solution. Often overlooked is the need for a comprehensive training program. Training should not be limited to mere functionality of newly installed systems. Employees should understand the purpose of the new products and procedures through a review of PATRIOT Act regulations. They should be taught, for instance, how to identify suspicious customers and how to detect money laundering through use of their new systems and procedures, as well as visual evaluation. The more thorough the training program, the better-equipped employees at all levels will be to detect money laundering and fraud.

Continued Monitoring. Once the firm's employees are trained and its systems are in place, a continual monitoring program must be established. Firms need to monitor, for instance, the effectiveness of their anti-money laundering systems and procedures, changes in PATRIOT Act regulations, and developments in money-laundering and fraud techniques. Firms' procedures and systems will require enhancements based on changes in the AML environment. The U.S. Treasury Department will be maintaining tight deadlines for compliance with PATRIOT Act and AML regulations. Therefore, once a firm completes its initial implementation of an AML/PATRIOT Act solution, it must maintain the initial cohesive project environment. This will allow it to effectively and efficiently implement procedural and systems enhancements in a changing AML environment.

As noted earlier, full AML/PATRIOT Act compliance will require a continued commitment by firms to monitor and maintain an aggressive strategy and policy of compliance. Continued monitoring of compliance programs will be a firm-wide process requiring organization-wide commitment.

While individual firms may differ in paths chosen to comply with PATRIOT Act requirements, the basic tenets remain the same across the industry. Compliance requires an ongoing commitment, operationally, technically, and culturally, brought about through strict project management and expertise. Once firms recognize that compliance lies beyond individual technological, operational, or legal applications, and that it encompasses the entire firm complex, the right solution can be put in place.

About the Authors

Vincent Manning is a Managing Consultant at Venture responsible for providing leadership in the development and implementation of innovative solutions to solve complex technical and business issues. Vincent actively works with senior management teams to assess current business and systems environments and proposes organizational and process reengineering solutions.

Marc Spitzner is a Consultant with over nine years experience in compliance, securities and mutual fund accounting as well as technical expertise with a variety of client/server and web technologies.

Ralph Martin is a Partner at Bingham McCutchen LLP and a Consultant in Bingham Consulting Group. He is the former Suffolk County District Attorney, having served as the chief elected law enforcement official for Boston, Chelsea, Revere and Winthrop from 1992-2002.

Don Savery is a Partner at Bingham McCutchen LLP in the litigation area where he represents individuals and business entities involved in a wide variety of commercial disputes. He has represented clients in state and federal courts, as well as in alternative-dispute-resolution settings, including arbitrations before AAA and other ADR groups.

For additional information please contact Venture Financial Systems Group, LTD. at (781)-932-7544.