Anti-Money-Laundering Regulations: New Teeth, New Tools

by Rona Distenfeld

It's not a pretty picture when an individual or institution is caught with its guard down. There's the double whammy of being being defrauded and being nailed by fines—or worse—from not having the proper processes in place to guard against money-laundering activities. And technology tools are not without their own risks.

Recent regulations enacting Title III of the USA PATRIOT Act have focused new attention on anti-money-laundering (AML) compliance. Public enforcement actions—such as the Written Agreements between the Federal Reserve and several of its member banks, including HSBC, Banco Popular, and Southern Commercial Bank— specifically cite Bank Secrecy Act and related Due Diligence, OFAC, Customer Information Programs, Currency Transaction Report, and Suspicious Activity Report requirements. Therefore, any technology-based solution must be able to address all of these areas to be effective and provide the regulators with evidence that such a system is in place.

At the center of the new requirements is a heightened expectation of a bank's ability to identify its customers and understand their usual transaction routines. This starts with such basic steps as recording identification documents, such as a driver's license, when an account is opened. With more affordable and portable equipment for scanning the magnetic strips and/or bar codes that most of these documents now carry (and OCR machines for the few states that don't yet use either), more banks are making this the first step in their know-your-customer programs. Since driver's licenses are the most fraudulent document in use, the data captured from the magnetic strips and bar codes offers banks an early alert if the face of the document has been altered. However, this is just a first step in an effective AML program.

Finding Your Best Technology Solution

According to a recent American Bankers Association survey, AML is now the most expensive compliance cost in the bank. What you spend can range from the thousands into the millions, depending on your bank's needs. That's why it's critical to evaluate your bank's current business and capabilities, future growth areas, and existing technology before looking for specific technology solutions.

 Rona Distenfeld is a freelance writer from Austin, Texas.

"There is nothing in the BSA that specifically states that a bank must have an automated system," says Pamela (P.J.) Johnson, senior anti-money-laundering coordinator at the Federal Reserve Board in D.C. "However, according to our rules, a bank must implement a program that ensures compliance and must operate in a safe and sound manner. This includes being able to file the appropriate forms, identify suspicious activity, and maintain the required records and be able to produce them when requested within the required time frames. If a bank is able to do this effectively using a manual system, that's fine. The bottom line is a bank needs to have a system that is commensurate with its size, complexity, and risk. By the same token, simply having an automated system isn't enough if it doesn't do what's necessary to effectively manage the risk."

This makes it clear that any system must match your bank's actual activities and be backed by a reliable vendor that will keep it up-to-date with both changes to the rules and changes to your operations. Some community banks believe they face minimal AML risk due to their location or because they don't participate in high-risk activities. While this is true in theory, they still must be able to provide regulators and law enforcement agencies with requested records in a timely manner—72 hours if their records are subpoenaed.

Before AML became a hot button, most comprehensive programs required a mainframe, so they were available only to large institutions. Today that has changed. A growing number of companies—many of them new and a few, such as Atchley Systems Inc. and SAS, around for decades—now offer in-house or outsourced solutions to community banks. Long-term familiarity with this issue can be a plus in a vendor, especially for community banks that may not have the internal resources to keep their systems up with the latest changes.

CHOOSING THE WRONG SOLUTION OR TECHNOLOGY VENDOR CAN *INCREASE* A BANK'S RISK BY PROVIDING A FALSE SENSE OF SECURITY.

There are a lot of packages, and more are coming every day. You can buy something off the shelf, customize or develop something yourself, or outsource. So how do you determine what's best for your bank—or if you even need an automated system? And how do you choose the right technology partner for your needs?

Choosing the wrong solution or technology vendor can *increase* a bank's risk by providing a false sense of security. There's strong agreement among bankers, regulators, and vendors about the questions to ask when looking for your best AML technology solution:

1. Is a technology solution appropriate for my bank's activities?
2. Do we have the resources to develop and/or manage this function in house? Can we maintain and update an in-house system properly? Would outsourcing be a better solution?
3. Do we want to find a single vendor that can provide technology solutions for all the pieces (BSA, OFAC, KYC, CTR and SAR filing, etc) or do we want individual "best-of-breed" packages?
4. How much experience does the vendor have with AML—extensive, or is this a new offering? Is the vendor's background more in software or in banking compliance? Is there regular communication with the regulators?
5. How long have has the vendor been in business? Is the company financially sound? Is it committed to continuing to support and update AML products?
6. How well does the vendor understand my bank's critical business needs?
7. Can the vendor advise and support me in this area and help me train my people to use its program?
8. How often does the vendor update its software? Are updates driven by internal timetables or regulatory deadlines?
9. Is the vendor's technology capable of handling our needs? Will it integrate easily with our other systems and infrastructure?
10. Does the vendor have other customers like me, using my systems, and already understand the necessary interfaces?

EARLIER THIS YEAR KOREA EXCHANGE BANK OF NEW YORK WAS FINED $1.1 MILLION DOLLARS FOR MISTAKES AT A BRANCH WITH LESS THAN $83 MILLION IN ASSETS.

11. Does the system do more than generate CTRs or SARs? Does it use "fuzzy logic" to do such things as match names even if the spellings are slightly different (a favorite trick of money launderers)? Can it learn what is normal for individual accounts? Can I enter my own parameters for suspicious activity?
12. Do we have the resources to use all the things the system can do? Do we need them? Who will read all the reports it generates? How will we be alerted to suspicious activity?
13. Can I get references?

The sheer volume and complexity of criteria make an automated process the best answer for most banks. "Any bank with more than four or five branches will be dealing in volumes that would be difficult, if not impossible, to manage manually," says Brent Atchley, vice president of Atchley Systems Inc. "There's no question that the number of CTRs and SARs has exploded, and that's just the tip of the iceberg. AML compliance now has a much greater focus on activities that try to avoid triggering a CTR or break from a normal pattern of activity for that account holder. That's why [companies] have added the ability to spot this type of activity to [their] software. The output has led to indictments of criminal activity by law enforcement agencies."

Others in the industry agree with this assessment. "Many bankers still think compliance in this area is about reporting specific sets of transactions," says Ken Proctor of Alex Sheshunoff Management Services. "The real issue is being able to monitor suspicious activity. That means a customer identification program, efficient archival and retrieval methods, and the ability to research using changing criteria. In most banks this just can't be done manually any more."

Balancing Needs Against Costs and Consequences.

There are now increased risks of not having an effective system to identify changes from what is normal and expected for each customer as a way to flag suspicious activity. For example, earlier this year Korea Exchange Bank of New York was fined $1.1 million dollars for mistakes at a branch with less than $83 million in assets. FinCEN's Assessment of Civil Money Penalty made the requirements clear:

"To comply with the SAR rule, a financial institution must be able to determine whether transactions are in fact reportable. Therefore, a financial institution is required to have in place systems to identify the kinds of transactions that may be a high risk for money laundering or that exhibit indicia of suspicious activity, taking into account the type of products and services it offers and the nature of its customers. Otherwise, a financial institution cannot assure that it is in fact reporting suspicious transactions as required by the BSA."

This puts pressure on banks to use profiling tools to mitigate their risk. To be effective, policies and procedures must be enforced, and any technology solutions must be monitored and the information produced must be acted on. Banks can't simply pass the burden of risk on to technology providers, even if they outsource the processing.

"Money launderers don't walk in the bank with suitcases full of cash anymore," says a Houston banker. "They start out looking like "A" credits; then, sometimes years later, they suddenly become "B" credits. You absolutely have to have a system that uses some type of artificial intelligence to take a profile of each customer so it can look for changes in their patterns and alert you."

The Houston banker is quick to point out that not all activity designed to evade reporting is motivated by criminal activity. "Some people will avoid the $10,000 mark just because they don't want to spend time filling out the form. It doesn't mean they're crooks, and they probably don't even realize that intentionally structuring their transactions to avoid the report is a crime. Your system still has to be able to spot the activity and alert you so you can investigate."

Johnson from the Fed agrees. "You can't just plug the system in and let it run. You still need people to evaluate, analyze and investigate the information. That's why it's important to identify and understand your customers—if Ms. Jones suddenly starts moving hundreds of thousands of dollars from savings to checking and spending it after years of small deposits and withdrawals, it doesn't necessarily mean she's doing something illegal. Maybe she just bought a house."

Failure to comply can be costly. For example, violation of OFAC requirements may involve criminal violations resulting in corporate fines up to $1 million, personal fines up to $250,000 and up to 12 years in jail. Civil penalties may be imposed as well in amounts up to $275,000 per violation. Noncompliance with other parts of the BSA may be equally severe. Beyond the fines, the cost of bringing the bank into compliance after the fact can be huge. For example, as part of its Written Agreement HSBC must go back and review all of its past transactions for one year, looking for cases that should have triggered a SAR. Once this is done they must go back even further.

"This is a risk and you need to approach it like any other operational risk and make the necessary investment," says Mark Moorman, vice president of the Financial Services Practice for SAS. "Government is dead serious about this and you don't want to be the person they use to send the message. Even if something terrible does happen, the fact that you did everything you could to prevent it will give you a lot of ground to stand on."

Johnson sees an upside to the increase in automation. She says banks sometimes use the information they get from their monitoring systems to track product usage and market their services more effectively. And she sees them doing a good job with a tough issue. "Managing risk is a very tricky thing. Most banks have done a tremendous job with this issue. Only a small percentage of banks have problems serious enough to warrant a public enforcement action, that is the good news. We expect that banks will integrate these new requirements into their existing systems and programs in the same manner." ❐

Distenfeld can be reached at rona@sbcglobal.net.

Maximum OFAC Penalties Per Transaction Violation
Years Imprisonment and/or Fines

OFAC Laws	Civil Penalties		Criminal Penalties	
	Individual	Corporate	Individual	Corporate
Trading with the Enemy Act	$55,000	$55,000	10 years + $250,000	10 years + $1 million
International Emergency	$11,000	$11,000	10 years	10 years
Economic Powers Act	$250,000	$500,000		
Iraqi Sanctions Act	$275,000	$275,000	12 years + $1 million	2 years + $1 million
United Nations Participation Act	None	None	10 years + $250,000	10 years + $500,000
Cuban Democracy Act	None	None	10 years + $250,000	10 years + $1 million
Cuban Liberty and Democratic Solidarity Act	$55,000	$55,000	10 years + $250,000	10 years + $1 million
Antiterrorism and Effective Death Penalty Act	N/A N/A	N/A N/A	The greater of 10 years + $500,000	$50,000 OR 2 times and the amount that should have been blocked plus $250,000
Criminal Code	None	None	5 years	$10,000