FIBA conference highlights key BSA/AML concerns

Learn latest AML trends and areas of regulatory focus

Read our white paper of highlights from the 2016 FIBA conference for BSA/AML insights banks can use today.

The following highlights from the 2016 Florida International Bankers Association (FIBA) conference offer guidance to banks on where to focus their anti-money laundering (AML) efforts in light of tight and evolving regulatory attention.

Lessons learned from enforcement actions

Regulators can use a variety of enforcement actions in Bank Secrecy Act (BSA)/AML cases. Informal actions, which are not publically available, include memorandums of understanding and Part 30 compliance plans. Formal actions include cease and desist orders (C&Ds), written agreements, civil money penalties (CMPs) and criminal prosecutions. In 2015 and 2016, the Office of the Comptroller of the Currency (OCC) actions included:

- Six C&Ds: three at large banks, one at a regional bank, one at a savings and loan and one at a federal bank branch
- One written agreement with a federal bank branch
- Three CMPs
- 31 formal actions are currently outstanding, but not yet fully addressed
- Nine informal actions are currently outstanding

For financial institutions, the key issues are what triggers an enforcement action and how to avoid them. Common issues resulting in enforcement actions fall into three categories:

- Internal control weakness – including incorrect or ineffective customer risk rating methodologies, failure to obtain and verify Customer Identification Program (CIP) documentation, failure to subject foreign affiliates to normal customer due diligence (CDD) or enhanced due diligence (EDD) procedures and insufficient documentation of CDD or EDD
- Transaction monitoring and suspicious activity reporting (SAR) issues – including relying on a manual transaction reporting system or a system that the institution has

otherwise outgrown; data issues, usually stemming from ineffective consolidation or assimilation of acquired entities; model validation issues; and "managing" alerts (e.g., capping the number of alerts to match available resources in order to ensure that alerts are addressed in a timely fashion)

- Other general governance issues — including an unqualified compliance officer, failure to maintain independence between the compliance officer and business lines, an audit that is too narrow or that is conducted by a party that lacks independence or technical expertise, ineffective or infrequent training, insufficient BSA/AML resources, an ineffective board that fails to provide oversight and failure to implement an entity-wide BSA/AML program

By paying attention to key BSA/AML program issues, financial institutions can strengthen their compliance programs and minimize the likelihood of an enforcement action. Focus on these key issues:

- Build a culture of compliance across the institution and with a strong governance focus, including support from and involvement of the board and senior management.
- Don't let your BSA/AML compliance program be conducted in a silo—include representation from throughout the bank, including new product development, your information technology (IT) department and your various product and service lines.
- Ensure thorough CIP, CDD and EDD policies and procedures that include an effective assessment of customer risk and solid know your customer (KYC) efforts at the relationship, not just the account, level. Incorporate front-end knowledge and understanding of your customers into your transaction monitoring.
- Ensure solid reporting, including researching and documenting the disposition of alerts on a timely basis; timely reporting of any suspicious activity; and periodic validation of your transaction monitoring systems.
- Choose and effectively implement the right systems. Use your own test data when evaluating systems to enable a full assessment of their capabilities and reporting—don't rely on canned sales pitch materials. Maintain a transaction monitoring system that is commensurate with the size and complexity of your bank.
- Build the right team. Make sure you have sufficient—and sufficiently experienced—professionals on both your BSA/AML compliance and on your audit teams. Larger institutions may need a dedicated team of IT professionals supporting their BSA/AML effort. Have a succession plan in place for key personnel.
- Maintain an effective and honest relationship with regulators. Ask questions when necessary and admit to shortcomings instead of trying to hide them. It is far better to work with regulators toward a solution than to be caught hiding something. If remediation is required, ensure strong governance over your remediation plans:
  - Develop training and communications plans early
  - Provide effective project management and management of information systems (MIS) reporting
  - Develop a reasonable and feasible action plan that includes all required actions and sets reasonable timelines
  - Define clear lines of accountability
  - Develop standards for evidencing and sustainability of the new process
  - Include testing to validate completion of action plans prior to next regulatory examination
- Work with consultants effectively. If you use outside consultants, define their role. Are they independent or an extension of management? Remember, you still own the work, so you have to ensure proper oversight, including of any outsourced functions

For more information on handling enforcement actions, read our articles 7 steps: How to respond effectively to an AML enforcement action, and 3 ways to realize ROI on your AML enforcement action response.

What's new in the AML landscape?

Regulators continue to emphasize the need for effective BSA/AML program governance and the central role that a comprehensive, effective risk assessment process has to play. Following are some key insights from this session:

- Oversight of your risk assessment process by senior management and your board of directors is vital. They should ensure not only that your risk assessment covers your full range of risks and is tailored to your institution's risk tolerance, but also that your BSA/AML program has sufficient resources to act effectively.
- Be sure to have effective escalation policies and procedures in place. These should include specific event triggers and follow-up responsibilities.
- Documentation is vital. All BSA/AML decisions should be documented. The more significant the decision, the greater the level of support you should have for it
- Your BSA/AML program and your risk assessment need to keep up with changes in technology within the bank. Banks can have multiple systems generating information on the same customer, which can lead to inaccurate or incomplete data mapping and monitoring. Be sure to accurately integrate data from across your systems to form an accurate picture of customer activity.
- Refine your risk assessment practices to keep up with new trends in technology and services like remote deposit capture, Society for Worldwide Interbank Financial Telecommunication (SWIFT) transactions and bitcoin.
- On the horizon? Global networks that will allow banks to transact directly with each other without an intermediary. That will increase efficiency, but also increase risk. Keep in mind that regulation always trails technology, which heightens risk until regulation catches up.

- Financial institutions are increasingly targeted by cybercriminals. Be sure to include any cyberattacks in your SARs—and include IP addresses. Consider voluntarily sharing appropriate information about these attacks with other financial institutions under the safe harbor provided by Section 314(b) of the USA PATRIOT Act.

For more information on effective risk assessments, see Using a risk assessment to clarify your AML picture. For an overview of key AML/BSA best practices, download our white paper, Seven key AML areas to focus on today.

Broker-dealers' AML compliance

Regulators continue to tighten BSA/AML compliance focus on broker-dealers. Key emerging issues include broker-dealers providing bank-like products without adapting their AML programs to comply with regulatory requirements (e.g., failing to file currency transaction reports and not adapting their monitoring systems to trigger alerts). Regulators are also focusing on cash balance accounts with little or no brokerage activity.

Following are key questions driving exam priorities for the Financial Industry Regulatory Authority (FinRA) and the Securities and Exchange Commission (SEC):

- Are SAR filing practices consistent with a broker-dealer's business model?
- Are SARs tested independently?
- Is the broker-dealer addressing exam results?
- Was the independent audit conducted by qualified parties?
- Is the broker-dealer applying a risk-based approach to its BSA/AML practices by using findings from previous examinations, considering current hot BSA/AML issues, and appropriately considering risk topics applicable to its unique business model and customers?
- Does the broker-dealer have appropriate escalation procedures in place to address SARs or other issues?

FinRA also outlined issues that should raise red flags for broker-dealers, including:

- Multiple accounts owned by individuals with common addresses in foreign locations
- Clients referred by individuals with regulatory histories
- Clients with long-term financial instability
- Clients with adverse media attention
- Recent stock promotions

FinRA also reminds broker-dealers to continue to be aware of possible abuse of senior citizens. FinRA has a hotline for reporting suspicious activity by caretakers or legal representatives of elder investors. Remember, there is a check box for elder abuse on the SAR.

For more information on BSA/AML compliance for broker-dealers, read our article, Investment advisors face new Bank Secrecy Act anti-money laundering rules.

SAR trends and issues

Financial Crimes Enforcement Network (FinCEN) serves as a vital source of information for other government agencies in their efforts to combat financing of terrorism and other financial crimes. SARs provide key information to support that effort. Therefore, timely and accurate SARs are important tools for law enforcement.

FinCEN reports an increase in SAR filings for 2015. The following tables provide an overview of the volume of filings by type of institution and by the top 10 states.

Filings by institution type

Industry	SAR filings
Depository institutions	2,543,299
Money services businesses (MSBs)	2,071,289
Casinos and card clubs	127,155
Securities and futures industries	59,724
Insurance companies	9,207
Other	135,194
Loan or finance companies	1,590
Housing government-sponsored enterprises (GSEs)	1,428

Top 10 reporting states

State	SAR filings	Percentage of SARs filed
California	434,840	14.46%
New York	288,452	9.59%
Ohio	240,079	7.98%
Texas	255,984	7.51%
Florida	185,738	6.18%
Delaware	134,485	4.47%
North Carolina	126,586	4.21%
Virginia	106,438	3.54%
Illinois	95,634	3.18%
New Jersey	87,165	2.90%

Some of the most common types of fraud or other suspicious activity for 2015 were:

- Tax refund or other tax fraud
- Check kiting and credit card kiting
- New account fraud
- Deposit fraud
- Prepaid card fraud
- Income and employment discrepancies
- Identify fraud
- Fraud rings

Two particular areas with a high concentration of SAR activity include MSB customers of federal credit unions and employment-based fifth preference visa (EB-5) investors. Due to risk issues and negative publicity, the majority of large and mid-sized commercial banks stopped taking MSBs as customers. As a result, federal credit unions have hundreds of clients who are MSBs, check cashers or foreign exchange houses that remit or receive hundreds of millions of dollars to and from jurisdictions such as Latin America, Asia, the Middle East and Africa. Credit unions with such customers need to ensure that their risk assessments and BSA/ AML programs accurately address these relationships.

Foreigners, primarily from China, are investing billions of dollars in U.S. real estate, hoping that they will be able to secure green cards through the EB-5 program. In some cases, though, wires from these investors are funneled through bank accounts in different states in order to make it appear that the investments are coming from bank account holders. These account holders are often college students. A significant number of SARs stem from this sort of funneling activity.

How to file a better SAR

FinCEN has seen a decrease in the accuracy and data quality of the information provided on SAR forms. Some common issues include:

- Missing RSSD numbers (SARs and CTRs)
- Failure to complete the entire form
- Inadequate or incomplete narratives
  - Failure to explain the nature and circumstance of the suspicious activity
  - Narratives that contain tabular account data
  - Blank narratives
  - Narratives that contain caveats, legal disclaimers or a template

These data quality issues make it difficult for FinCEN to analyze the exact nature and reasoning for the SAR. When filing a SAR, be sure to include the following:

- The origin of the money and where the money is going
- Supporting details that provide an analysis of the transaction in question

Sanctions compliance

Evolving geopolitical realities are complicating compliance with Office of Foreign Asset Control (OFAC) sanctions for many financial institutions. Banks must be sure to back up both specific transaction decisions and their risk analysis involving any customers potentially subject to OFAC sanctions with solid documentation.

The three main areas of risk for sanctions compliance are:

- Trade finance
- Correspondent banking
- Transaction monitoring

Easing of sanctions against Cuba, Iran and Burma make compliance more difficult for transactions with parties in or involved with these countries. Where many of these transactions would previously have been banned outright, financial institutions now must exercise effective judgement. Given its proximity to the U.S., understanding the situation in Cuba is especially important. The trade embargo is still in effect, though some exports to Cuba are permitted. Currently, U.S. banks can open accounts at Cuban banks for the sole purpose of processing program-permitted transactions, including credit card transactions for U.S. persons travelling in Cuba. U.S. travel service providers can arrange for U.S. persons to travel to Cuba, and banks can rely on the traveler to attest that travel was permitted unless the bank has reason to believe otherwise.

Russia also faces sanctions due to its invasion of the Ukraine. Russia is moving illicit funds through financed assets, such as real estate and boats. Banks are at risk for loss should they accept those assets as collateral and the assets end up being seized. Banks should also place the names of cities and ports in the Crimean region in their OFAC screening databases. SARs involving Russia or the Ukraine should be reported to the OFAC as well as FinCEN.

Geographic targeting orders (GTOs) are the latest tool that FinCEN is using to combat money laundering and other financial crimes. A GTO imposes certain additional reporting and recordkeeping requirements on one or more domestic financial institutions or nonfinancial trades or businesses in a specified geographic area. If your institution is subject to a GTO, tailor the basics of your BSA/AML risk management and other processes to comply with the GTO, with an emphasis on customer due diligence.

+1 800 274 3978
www.rsmus.com

tl-se-con-fi-0416