A review of the Florida International Bankers Association 13th Annual Anti-Money Laundering (AML) Compliance Conference

Prepared by:

Christopher Dick, CFE, CAMS, *Manager*, McGladrey LLP
305.569.7974, chris.dick@mcgladrey.com

Lianet Cicero, CPA, *Associate*, McGladrey LLP
305.569.4181, lianet.cicero@mcgladrey.com

Tracy Coykendall, *Associate*, McGladrey LLP
305.446.0114, tracy.coykendall@mcgladrey.com

Erika McCormick, MBA, *Supervisor*, McGladrey LLP
703.336.6400, Erika.mccormick@mcgladrey.com

Norma Penate, CAMS, *Supervisor*, McGladrey LLP
305.446.0114, norma.penate@mcgladrey.com

April 2013

Background

The Florida International Bankers Association hosted its 13th annual Anti-Money Laundering (AML) Compliance Conference in Miami on Feb.13–14, 2013. The conference attracted a record number, with more than 1,300 industry professionals from throughout the United States and abroad gathering for two complete days of sessions around AML and Bank Secrecy Act (BSA) compliance topics.

What follows is a summary of several of the sessions from throughout this year's conference. This document is not intended as an exhaustive review of the entire conference. It is a high-level synopsis of several of the topics that are of interest to banking professionals.

General session: What's new in the AML landscape?

The opening session of the conference featured a panel of representatives from the banking industry and representatives from federal banking regulators and other agencies. The discussion covered a number of topics, including modernization efforts of the Financial Crimes Enforcement Network (FinCEN) and the new electronic Suspicious Activity Report (SAR) and Currency Transaction Report (CTR) filing processes, the status of the advance notice of proposed rule-making regarding Customer Due Diligence (CDD) and beneficial ownership, and regulator expectations for BSA/AML compliance programs in the wake of recent record penalties imposed on HSBC, JP Morgan and Standard Chartered, among others.

Industry representatives focused largely on the steadily increasing expectations and demands placed on BSA/AML compliance departments, coupled with increasing penalties for non-compliance. The new electronic

CTR and SAR forms and batch filing processes have posed technical challenges for some institutions. Despite government claims that the new forms do not impose any new requirements, they include a number of new fields. Financial institutions will also have to modify the manner by which they collect information to complete these forms properly. The inclusion of a number of new categories of reportable suspicious activity underscores the increasing convergence of efforts to combat additional types of financial crime, such as fraud, tax evasion and corruption, in addition to the traditional areas of money laundering and terrorist financing.

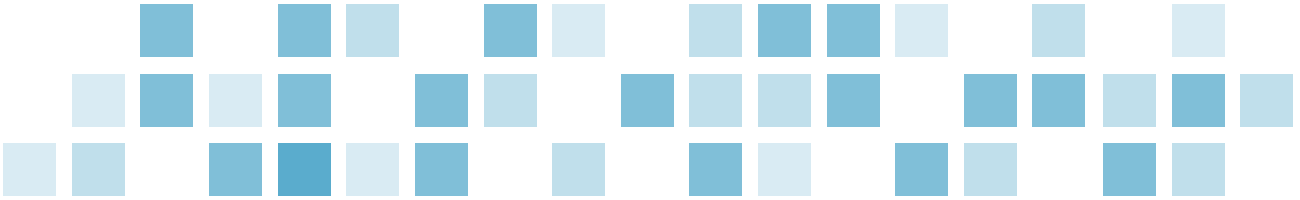
On the topic of the proposed CDD and beneficial ownership rules, industry representatives stressed the need for clearly defined and realistic requirements. For many banks, procedures for customer due diligence and identification of beneficial owners have, to date, been a risk-based best practice, rather than a regulatory obligation. The representative from FinCEN stressed that their goal is not to reinvent the wheel, but instead to leverage existing practices that financial institutions have shared during that bureau's information gathering process. The goal of the new rule is to level the playing field between banks that currently have strong CDD procedures and those that do not, through clearly defined rules and expectations. In addition, the new rules will be released well in advance of the effective date to allow for needed adjustments to compliance programs.

Another theme of the discussion was the need to refocus on the basics of AML compliance. Roles and responsibilities for compliance need to be clearly defined across the organization, particularly with the launch of new products or entry into new geographies. This was echoed by comments from regulators on the panel, who noted that many of the recent enforcement actions that have received publicity have involved failures of basic BSA/AML controls. Matters requiring attention (MRA) in recent examinations have dealt with fundamental areas of control, such as documentation of transaction monitoring and sanctions filtering thresholds, gaps in coverage of sometimes entire divisions or product lines, and failure to adequately assess BSA/AML risks.

Representatives from the OCC and the Federal Reserve Bank stated that upcoming examinations will pay particular attention to the enterprise-wide policies and procedures and the operational environment of the BSA/AML compliance program. Banks should have incentives in place in terms of compensation and accountability to align further the interests of the Compliance and Business lines. Boards of directors and management should work together with Compliance to ensure a functioning BSA/AML program. Financial institutions also need to ensure that the BSA department staff has adequate expertise and resources. In addition, the BSA department should have adequate access to senior management and the board of directors.

Panelists also focused on the importance of having an enterprise-wide BSA/AML compliance program. Banks are expected to have an enterprise-wide risk assessment, policies and procedures. It is critical that processes are in place to share information across business lines and jurisdictions within a financial institution. Transaction and sanctions monitoring systems should also be appropriate for the size of the institution. Regulators have noted a number of institutions that have grown rapidly through acquisition, where the systems were not sufficiently upgraded. Regulators will not approve acquisitions for financial institutions with serious BSA/AML deficiencies.

Lastly, the panel addressed the impact of increasing BSA/AML requirements on community banks. Regulators on the panel stated that community banks will be held to the same standard as larger banks, while noting that the fines on smaller institutions have a far greater impact than the much larger recent penalties on large banks. Regulators are finding issues related to third-party payment processors, ACH clearing and foreign correspondent banking, as smaller institutions branch out into new products and services, often without proper risk assessment and controls. The panelists recommended that community banks reach out to larger banks with questions and ask for recommendations on best practices.



Compliance culture and the role of the compliance officer: Who owns the risks?

This presentation focused on the role and responsibilities of a compliance officer and the panel consisted of representatives from financial institutions and business advisory firms. The overall theme was that in today's environment, compliance officers need to be a "Renaissance people," who is able to juggle the competing interests of the board of directors, regulators, business line management and their own departments. At the same time, they must have a broad vision and strategy for the compliance department's efforts, because a myopic approach will increase the risk of non-compliance.

Compliance officers' responsibilities include identifying regulatory requirements, assessing the organization's level of compliance, ensuring accurate reporting, reviewing exceptions to the compliance program and addressing any gaps or weaknesses. The responsibility of the board and management is to provide the necessary support, resources and cooperation for this individual to carry out his or her duties.

A common but significant issue is a lack of understanding of a compliance officer's role within an organization. BSA/AML compliance requires more than focusing on the minimum statutory requirements; it requires the compliance officer to actively manage risks. This entails continual assessment of changes in business practices within the organization, changes in the industry and changes in the regulatory environment. A compliance officer should consider the organization's future compliance framework by reviewing emerging regulations and determining their impact. Another key area of risk management is to develop tools that ensure the compliance officer has an adequate understanding of where the organization's risks lie. Data analytics can be an effective tool to identify and even predict risk; however, it is important to verify that the data is accurate and comprehensive.

Compliance officers must engage management and the board to manage risks effectively. This person should have the authority and stature within the organization to challenge existing processes and introduce new best practices. A compliance officer should have direct access to the board and reports of deficiencies should be taken seriously by the board to ensure needed changes are made. This helps to develop a strong culture of compliance within an organization and demonstrates that everyone in an organization has a responsibility and a role in compliance. Best practices for tracking or measuring the culture of compliance include periodic discussions or interviews with staff throughout the organization to measure the effectiveness of training and to identify ongoing issues or concerns. Tracking and reporting of compliance metrics to the board can also demonstrate the level of commitment to compliance by the business line.

Concluding comments by the panelists summarized some other key roles of a compliance officer. It is important to be able to adapt quickly to regulatory changes. The ability to communicate effectively is critical. A compliance officer must be able to maintain open and honest lines of communication with regulators. This person should able to express concerns, articulate risks and advocate for his or her position to the board and management in a clear and concise manner. Moreover, this person needs to communicate the importance of compliance to the entire organization.

Correspondent banking: Staple of the financial system or a shadow?

This presentation focused on the risks posed by foreign correspondent banking and best practice recommendations from regulators and industry representatives. The panel opened by discussing the many risks of foreign correspondent banking—the key risk being that the respondent bank does not control for AML risks to the same degree as the U.S.-based correspondent. In addition, the transaction monitoring process

often focuses more on the customers of the customer, adding a degree of difficulty to the due diligence process. Other challenges include high volumes of activity, the increasingly global nature of respondent and correspondent relationships, and difficulties in obtaining explanations and supporting documentation for transactions. Potential concerns about the foreign financial institution include corrupt or unsatisfactory management, lack of regulatory oversight and inadequate controls.

Regulators have focused heavily on foreign correspondent banking risks. Their concerns focus on due diligence standards, including limited identification of beneficial owners, failure to define expected activity types and volumes and due diligence that is not commensurate with the customer's risk profile. Foreign branches and affiliates should be treated as customers and subject to appropriate risk-based due diligence. These relationships should not be exempted from CDD procedures because of common ownership. Finally, regulators have placed particular emphasis on sanctions monitoring processes and controls.

The degree of enhanced due diligence (EDD) performed should be guided by a comprehensive risk assessment of the customer. Factors to consider should include jurisdiction, regulatory regime, reputation of management and owners, strength of AML compliance program, customer base, products and services to be used and expected volume of activity. USA Patriot Act Section 312 mandates an EDD program for foreign financial institutions (FFIs), with offshore banking licenses or license issued by a jurisdiction designated non-cooperative by FATF or subject to special measures under USA Patriot Act Section 311.

The panel discussed a number of recommendations for mitigating correspondent banking risks. The Wolfsberg Group AML Principles for Correspondent Banking was recommended as a good starting point for developing enhanced due diligence procedures, including: reviewing background and reputation of ownership and management; identifying any politically exposed persons (PEP) in management or ownership and determining their level of control; assessing the quality of the customer's AML program; and reviewing downstream correspondent activity to understand your customer's customers and determine the potential for nested activity. One panelist recommended questioning why a high-volume customer of an FFI would process transactions through the foreign financial institution, rather than open an account at a U.S. bank, citing this as a potential red flag. All panelists stressed the importance of involving the BSA department in the decision-making process when entering into foreign correspondent banking or when opening new relationships, and having open lines of communication between compliance and business line functions. The on-boarding process should be considered as much a compliance decision as a business decision, and panelists recommended establishing regular opportunities for dialogue between the compliance and business functions to discuss issues and find ways to overcome challenges.

Regulators on the panel provided insight into the areas of focus during examinations. It is expected that banks will have a strong foundation of policies and procedures that include having a written correspondent banking agreements; defined standards for customer acceptance and due diligence; and established parameters for activity and an understanding of the basis for the parameters. It is generally expected that FFI customers undergo annual due diligence reviews and that owners controlling 10 percent for high risk and 25 percent for low and moderate risk are identified. Regulators also place a heavy emphasis on having appropriate expertise within the BSA department and a tailored training program for all employees. The panelists also stressed the importance of comprehensive independent testing that should include review of due diligence processes, transaction monitoring and investigations, and ensuring agreements and certifications are in place.

Panelists concluded by discussing future trends. The increasing sanctions burden, particularly with regards to Iran and Syria, is creating additional risks for banking FFIs, and increases the importance of understanding

the customers of the customer. The growth of non-traditional banking products, such as virtual currency and mobile banking, are reducing transaction transparency. Finally, the increasing regulatory burden is creating risks and opportunities as the cost of compliance increases, driving some U.S. banks out of the market, providing growth opportunities for other banks.

Managing risks in international public/private partnerships: Is governance the answer?

This session focused on public/private partnerships (PPPs) to increase participation of the unbanked and under-banked in the financial system, and the impact of these efforts on an institution's AML risk. The session began by defining PPPs as partnerships that are "government service or private business ventures funded and operated through a partnership of government and one or more private sector companies." PPPs involve a contract between a public sector authority and a private party; typically, a public sector consortium forms a special company called a Special Purpose Vehicle to develop, build, maintain and operate an asset, including services, for a contracted period. These partnerships can create beneficial social change on a large scale.

The PPPs implemented by the U.S. Agency for International Development (USAID) in Colombia were highlighted during the discussion. USAID is active in many countries in Latin American, Africa and Asia, such as Peru, El Salvador, Colombia, Ecuador, Liberia, Ethiopia, Albania and Serbia. The programs in place in Colombia were elaborated on, but it was stressed that similar programs are in place around the world. Objectives in Colombia include promoting the expansion of private financial institutions in underserved areas, enhancing small- to mid-sized business activities, and providing access to justice programs.

One program currently in place encourages lending to small and mid-sized businesses. These loans are typically between $1,500 and $2,500; however, the maximum amount the program will permit is $100,000 per borrower. The program works off of the volume of loans, making many small loans through micro-institutions. The U.S. Government will locate potential partnership institutions and perform due diligence on the institution. Once the institution is selected to participate in the partnership, the institution is then responsible for performing know your customer(s) reviews or consumer due diligence for local borrowers. USAID allocates the risk of each loan evenly between the U.S. Government and the partnership institution; 50 percent of all defaulted loans are covered by USAID. The program targets vulnerable populations usually without access to financial institutions, including rural and post-conflict areas. The most common business funded through these loans is small farms.

Another PPP operating in Colombia works to provide access to justice programs. The partnership has established over 60 "justice houses" in isolated areas. These houses provide dispute resolution at local levels, targeting the Afro-Colombian and rural populations, as well as post-conflict areas of the country. The idea is for individuals to use these houses, staffed with prosecutors, to try to resolve issues related to domestic violence, gang violence or displaced persons. The hope is for these justice houses to evolve into more formal systems in the future. These houses will serve as drivers of development over time. The development of a formal legal system will assist in the development of formal bank systems, including formal bank transactions. Formal banking systems will reduce the need for alternative banking systems, such as local loan sharks. This in turn is expected to reduce the potential violence associated with alternative systems.

The session also highlighted some of the barriers to entering financial institutions that exist in some countries. It was explained that the foundation of AML laws and regulations can create a barrier to entry because of strict ID requirements, limitations on amounts or frequency and exceedingly demanding information requests

required by institutions in certain jurisdictions. Examples of barriers to entry include supervisory agencies in Nicaragua requiring a potential customer to provide a fixed phone line to open a bank account; however, there are approximately 5 million people in Nicaragua and only 150,000 fixed phone lines. This contributes to a large under-banked and unbanked population. Other countries, such as Mexico and Somalia, require customers to provide witnesses who will vouch for the individual prior to opening an account. Many countries continue to require reference letters from neighbors to open an account.

Panelists discussed the continued increase in remittances sent through financial institutions. Remittances can serve a valuable role in many countries, leading to an increase in disposable income and liquid assets. Remittances lead to financial inclusion, access to financial systems and wealth generation to increase financial independence. The AML concern for remittances was discussed. Due to the normally low amounts, the risk is not substantial. Typical money launderers will launder between $20,000 and $100,000, which is usually outside the range of remittances.

Identification requirements were then addressed. These requirements can be difficult for displaced persons, refugees and geographically isolated persons to meet. The question of how access to financial institutions can be expanded without reducing ID requirements was also addressed. Mobile and telephone banking can offer greater opportunities to expand access to financial systems, as well as prepaid cards. Laws and regulations surrounding these products must be enhanced.

Finally, financial institutions must remember it cannot be assumed that under-banked or unbanked customers are inherently low-risk. Risk assessments must be completed for each such customer to adequately determine the risk posed to the institution. Efforts must be made not to marginalize displaced persons or drive them out of a formal financial system if unable to provide identification. The panel also discussed ways to lower current barriers to entry to the banking system. The principal corrective action utilized is to petition governments and agencies for legislative fixes to change antiquated laws and establish equal access to financial institutions.

The new SAR form: Confidentiality issues and joint SAR filings

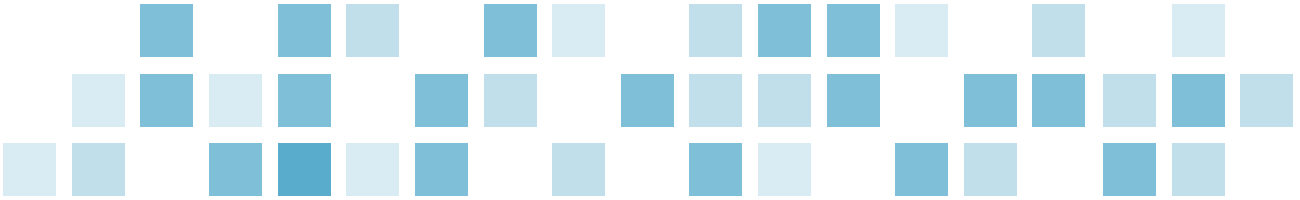
This session focused on the new suspicious activity report (SAR) form, the protection of SAR confidentiality, the criteria for when a joint SAR filing is permitted and the use of SAR information. The panel included speakers from the regulatory and industry perspectives.

The Office of the Comptroller of the Currency (OCC) issued the final rule governing the confidentiality of a SAR on Dec. 3, 2010 (75 FR 75576). Key components of the rule were to:

- Clarify the scope of the statutory prohibition on the disclosure by a financial institution of a SAR, as it applies to national banks
- Address the statutory prohibition on the disclosure by the government of a SAR, as that prohibition applies to the OCC's standards governing the disclosure of SARs
- Clarify that the exclusive standard applicable to the disclosure of SAR, or any information that would reveal the existence of a SAR, by the OCC is to fulfill official duties consistent with Title II of BSA
- Modify the safe harbor provision in the OCC's SAR rule to include changes made by the USA PATRIOT Act

FinCEN also issued a concurrent final rule concerning SAR confidentiality on Dec. 3, 2010 (75 FR 75593).

The panel discussed the differences among SAR documentation, SAR information and SAR supporting documents and the context in which the information can be shared, and is protected under the final rule. SAR



information is the SAR document or any information that would reveal the existence of a SAR, and therefore, is protected from disclosure. Under the final rule, banks and financial institutions are prohibited from sharing SAR information. If the bank or financial institution is subpoenaed or requested to share SAR information, the request is to be declined and the request is to be communicated to both the OCC and FinCEN.

SAR supporting documents, which are the documents and facts that may identify suspicious activity, have limited confidentiality protection under the rules of construction (12 CFR 21.11(k)(ii)).

The panel discussed the following challenges with SAR confidentiality:

- Presenting SAR data to a bank's board of directors
- Requests from secondary examiners
- Subpoenas for employee testimony in a civil litigation
- Balance need to know with front-line staff
- Employee SARs that do not involve joint filing
- SAR attachments in the new forms
- Malicious SAR filing and impact to the safe harbor provision

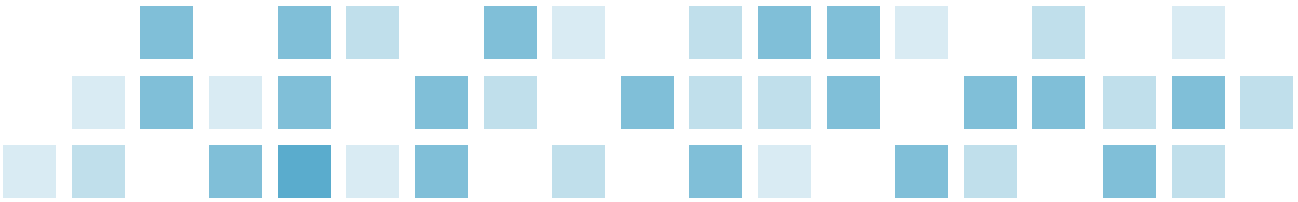
FinCEN issued FIN-2010-006 to provide guidance for sharing SARs with affiliates. The guidance states that an institution is permitted to share a SAR with affiliates that are subject to the SAR rule. The guidance also states that a U.S. branch of a foreign bank may share a SAR with its head office; similarly, a U.S. bank or savings association may share a SAR with its controlling company, whether domestic or foreign, to promote compliance with applicable requirements of the BSA and facilitate enterprise-wide risk management. Policies and procedures should be in place to ensure that affiliates protect the confidentiality of the SAR.

The panel emphasized that SAR sharing is permissible when the affiliated institutions are a bank, a broker-dealer, a mutual fund, a futures commission merchant or an introducing broker in commodities and the guidance is not expanded to authorize additional industries to share SAR information. In addition, SARs and the supporting documentation may be shared with law enforcement, a bank's primary federal regulator and FinCEN.

Financial institutions subject to SAR filing requirements may satisfy their SAR obligations by jointly filing a SAR. This includes banks and foreign-located money service businesses (MSB) doing business in the U.S. Joint filing reduces the number of duplicate SARs filed for a single suspicious transaction and the underlying facts, transactions and documents upon which a SAR is based may be shared with another financial institution to prepare the joint SAR.

The panel discussed how to assess the goals and current challenges within a financial institution's SAR program. In addition, the panel stated that SARs provide financial intelligence to the intelligence communities, allowing them to effectively connect the dots in their investigations and follow the flow of illicit funds.

FinCEN issued FIN-2012-G002 to provide guidance for the filing of the new reports through the BSA E-Filing System. Effective April 1, 2013, the new SAR form must be used. There are no new obligations for filing institutions or changes to the existing requirements. The new SAR will include additional data elements to allow for more effective use of the information collected in the reports. The new SAR will also have certain fields marked as critical for filing purposes; this means that the BSA E-Filing System will not accept filings in which these fields are left blank. Other enhancements to the new SAR include fields related to Internet presence and the ability to accept single, comma-separated value attachments.



OFAC challenges

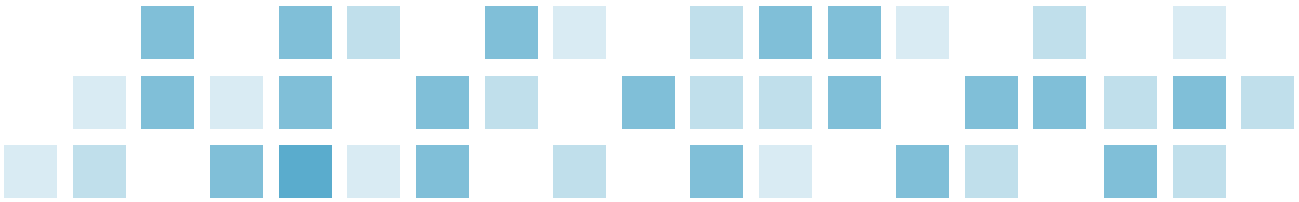
The Office of Foreign Assets Control (OFAC) issued a number of sanctions and actions during 2012; key acts include the National Defense Authorization Act of 2012 and the Iran Threat Reduction and Syria Human Rights Act of 2012. In January 2013, OFAC issued an advisory on the Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions against Iran. Similarly, OFAC has issued a number of civil penalties and enforcements during 2012, totaling approximately $1.1 billion in penalties and fines. There have been more than 200 enforcement actions since 2003. Notable enforcement actions include those against HSBC, Standard Chartered Bank and ING. These actions provided context in which the panel discussed the challenges facing OFAC enforcement, expanded coverage of sanctionable activities and lessons learned. Banks are also increasing the amount of self-reporting. When in doubt, it is in the bank's best interest to report the issue to OFAC. Self-reporting will always be viewed favorably by OFAC.

The panel discussed a few examples of OFAC issues, including a case study of a bank headquartered in Central Asia. This is a privately owned bank with no direct U.S. correspondent relationships; however, the bank has correspondent relationships with foreign banks in Russia and Germany that have U.S. relationships. A U.S. bank noticed more than 2,500 transactions throughout the past six years totaling $100 million, all of which originated from a single account at ABC Bank. The U.S. bank contacted six customers who received wires from that account; all customers confirmed the funds originated in Iran. The U.S. bank was able to determine that the account was an exchange house and all transactions were linked to Iran, although over 100 different ordering parties used the same account to originate payments. These payments referred to private transfers and inconsistent explanations were provided for these transfers. Different account numbers were then used after the U.S. bank began rejecting the payments. This scheme was caught by outstanding due diligence performed by the U.S. bank to uncover these deceptive, non-transparent practices by the non-U.S. bank.

OFAC investigations were subsequently discussed. Investigations can arise from a variety of sources, such as reports of blocked or rejected property, voluntary self-disclosures, ongoing/existing cases, referrals from other agencies, informants and other publically available information. If OFAC determines additional information is needed, it will be requested in accordance with 31 C.F.R. §501.602. Financial institutions may receive an administrative subpoena requesting additional documentation. Banks should not panic if such a subpoena is received; however, they should be prepared internally with adequate supporting documentation.

Following the investigation, OFAC will provide one of five response types. OFAC will always provide a response, even if the response is only verbal. If a response is not received, OFAC should be contacted; however, banks should be mindful that some investigations are lengthy. The least significant response type is that of No Action. The matter was investigated and no further action is required by either party. The second response type is that of a "Cautionary Letter." This type of letter is a warning to a bank to be careful in the future; however, the bank will not be subject to a penalty. The third response is a Finding of Violation. One such finding will not materially impact a bank; however, the finding will have implications for the future. Any future violations will be handled more severely, as they may be seen as repeat actions. The final two response types are Civil Penalty and Criminal Referral. Factors affecting the severity of findings include whether a violation was due to willfulness or recklessness, concealment by the financial institution, patterns of misconduct, prior notice and the level of management involved. The level of awareness surrounding the violation will also be considered. Actual knowledge, as well as reason to know, will be evaluated.

The panelists also stressed the need for financial institutions to cooperate with OFAC. The level of cooperation can have significant impacts on the consequences for any violations found. If an institution voluntarily self-



discloses, any future penalties that result may be reduced by as much as 50 percent. General cooperation without voluntary self-disclosure can result in a 25–40 percent reduction in penalty. The panel also noted the benefits to banks that can result in looking deeper into an OFAC issue. The results of the OFAC investigation may conclude that what appeared to be a violation is in fact not a violation. The statutory maximums for various types of violations were then discussed. A violation of the Trading with the Enemy Act can result in a $65,000 fine per count, while a violation of the Foreign Narcotics Kingpin Designation Act can result in a $1,075,000 fine per count.

Attention was then turned to the Iran Threat Reduction Act's (ITRA) implementation and challenges. The Act primarily affects institutions required to file SEC reports, and it requires institutions to obtain and report information related to affiliates. The disclosure requirements under ITRA were effective for annual or quarterly reports on or after Feb. 6, 2013. Covered activities taking place from Jan. 1, 2012 to Dec. 31, 2012 are to be reported. Reportable activity prior to when ITRA was enacted, and that the activity has been terminated, must be disclosed. The speakers stated that reportable activities have no materiality threshold or de minimus exception, and must include the nature and extent of the activity, gross revenues and net profits attributable to the activity and whether the issuer or affiliate intends to continue the activity.

The panel addressed the increased costs related to compliance and the culture of compliance and control required to have a successful program. Compliance officers are, more than ever, under significant pressures to satisfy increasing requirements. Senior management must be cognizant of this burden on the compliance function, and consider whether to invest additional resources on compliance controls, lower the risks the institution is exposed to, or figure out how to balance these two aspects

OFAC training requirements were then discussed. General OFAC compliance training is of course a requirement; however, additional training should be provided when needed. Banks may consider providing their foreign correspondents with enhanced training, including, but not limited to, personnel from the institution traveling to the correspondent to provide training. Other non-bank entities also require enhanced training, such as the securities firms.

Finally, the panel reminded attendees that, because a system was purchased to compare the database to the OFAC list, it does not mean the institution has fulfilled all OFAC requirements. Compliance with OFAC has challenges and is proven to be a balancing act. Institutions and firms need to consider whether to invest more on compliance controls or lower risk levels, and how to strike the balance between the two. Similarly, the expectations of managing regulatory risk and an economic sanctions compliance program remain high, and regulators will continue to expect sufficient resources and expertise to be given to the compliance function to manage risk and the scope and frequency of regulatory changes.

Mobile and e-payments

Mobile banking and e-payment services are a rapidly expanding area for both banks and non-bank financial institutions, providing new challenges to compliance departments, law enforcement and regulators. The panel consisted of representatives from U.S. and Russian banks and payment providers, and U.S. federal law enforcement. Mobile and e-payment transactions pose increased money laundering and terrorist financing risks because of the increased speed and anonymity they provide.

The panel first addressed key areas of risk and common controls that address these risks. They also stressed the importance of the financial institution understanding who has responsibility for compliance at each stage of the transaction. Panelists emphasized that compliance staff have an adequate understanding of how

the products work, the applicable regulatory regime(s) and the scope of compliance efforts related to these products. They also noted the importance of educating regulators on the new products to ensure they have a proper understanding of the risks and mitigating controls.

The general consensus is that mobile and e-payment products are high-risk; however, there are varying approaches to managing the risks. The panel discussed some best practices for customer due diligence and monitoring. The starting point should be traditional risk factors, such as geography and transaction volume. During the initial client on-boarding process, financial institutions should consider whether or not money is available before customer identification problem (CIP) is performed, and if CIP and CDD will be documentary or non-documentary. Ongoing controls should address limits on transactions, reload amounts, the number of cards sold to one person and if the product can be used internationally. Compliance departments should develop appropriate transaction monitoring, suspicious activity investigation and reporting processes that include fraud detection. Banks should also take care to ensure that fraud controls cannot be overridden by business line personnel.

Insight was provided into the booming market for mobile and e-payment products in Russia. The popularity can be attributed to rapid income growth combined with relatively limited access to traditional banks due to limited branch networks. Regulators are finding it difficult to keep with new payment providers that are joining the market on a regular basis. Nonetheless, many payment systems are run by traditional banks. Some recently launched products include microloans that can be disbursed via a remote lending terminal. The kiosk scans the borrower's passport and identity is confirmed through facial recognition software via the kiosk's video camera. The borrower completes the loan agreement and then cash is dispensed.

Another popular product is e-money or virtual currency. These services are similar to PayPal; the primary difference is that Russian e-money accounts are generally funded with cash. A specific law did not exist in Russia that regulates e-money until 2010. Regulations passed in 2012 on non-bank credit providers are similar to regulations adopted by the European Union. Customer due diligence requires face-to-face identification, and reliance on a third party, such as a regulated bank, is not permitted. Non-face-to-face verification requires notarized documents. Some e-money providers are exploring verification through online services such as Equifax; however, existing regulations do not permit reliance on this. The identification requirements are not risk-based or flexible; however, they only apply if customers transact more than 1,000 euros in a month or have an account balance exceeding 370 euros. Customers are able to use e-money services for day-to-day transactions, such as bill payment, online purchases, mobile phone minutes and taxes. Most customers do not have transaction volumes or account balances requiring full identification. The average account balance is 60 rubles, or about $0.20. As a result, the key risk control at this point is transaction limits.

Caribbean roundtable

Along with the concerns of building new schools, funding hospitals and/or trying to meet the basic needs of the populations, the Caribbean islands also face challenges in the endless battle against money laundering and terrorist financing. One of the recurring themes outlined in this presentation was the reputational risk the Caribbean islands face. Representatives from the Cayman Islands, St. Vincent and the Grenadines and Jamaica agreed that it has been difficult to change the global perception of the Caribbean being a high-risk money laundering area. The panelist discussed the areas of concern within their countries and the legislations that is being updated and/or implemented to enhance current anti-money laundering regimes.

The Cayman Islands representative shared key points in implementing the New FATF (Financial Action Task Force) 40 Recommendations, adopted and published in February 2012. The FATF Recommendations are the

basis on which all countries should meet the shared objective of fighting money laundering, terrorist financing and the financing proliferation. The FATF calls upon all countries to effectively implement these new measures in their national systems. The recommendations cover all the measures that national systems should have in place within their criminal justice and regulatory systems. The Cayman Islands implementation plan includes:

- National threat assessment
- Formally implementing a risk-based approach
- Effective supervision of DNFBPs (Designated Non-Financial Businesses and Professions)
- Effective sanctions and powers
- Domestic PEPs
- Proliferation

As a result of the new recommendations, changes in legislations, regulations and guidance may take place. The implementation may present resource challenges. It was mentioned that there is always a constant need to raise the bar and go "beyond minimum standards, while remaining competitive."

For St. Vincent and the Grenadines it has been a constant struggle to keep up with international standards and practice; nevertheless, the importance of developing and keeping up with updates is recognized. This country makes efforts to comply, in spite of the economic hardships the country faces. It was mentioned that there is no evidence of high money laundering in St. Vincent. There have been small cases of money laundering in the past. The most recent and the biggest money laundering case occurred in 2012. Two individuals were convicted with two charges of money laundering involving $1.7 million in cash. Training and awareness for anti-money laundering is rising.

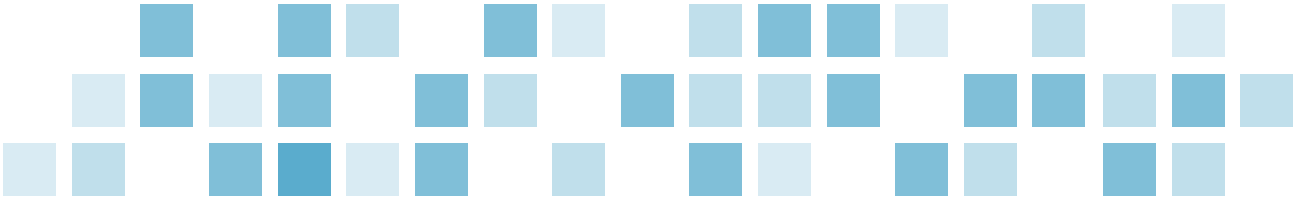
Panelists discussed key components of anti-money laundering in Jamaica. The Jamaican AML/CFT framework includes being a signatory of United Nations convention, terrorist convention and a member of the Caribbean Financial Action Task Force (CFATF). There are several pieces of legislation in place, such as the Proceeds of Crime Act 2007, The Prevention of Terrorism Act of 2005 and the Financial Investigation Division 2010.

A major concern in Jamaica discussed in the round table was the emerging risk of lottery scams. This is an area of significant concern and a fast-growing industry worth $300 billion. This scam is based on supposed lottery winnings being used to pry money from unsuspecting victims. Perpetrators call from the Jamaica-based 876 area code. Victims reside in New York, New Jersey, Florida, Maine, Vermont, New Hampshire and Hawaii. What the perpetrators call process fees are transferred by the victims to the scam operators via remittance companies. It is estimated that 30,000 calls are made each day to the United States by scam operatives. Lottoery scams have increased by 1,400 percent since 2007. It is estimated that only 10 percent of the victims report losses.

Mitigating international money laundering risks

This session focused on steps to identify and mitigate the risks of money laundering across national borders, and the need for institutions to establish and maintain effective Anti-Money Laundering (AML)/Office of Foreign Assets Control (OFAC) controls and systems. The panel included speakers from the regulatory and industry perspectives.

The panel identified the following examples of ongoing international money laundering concerns and areas vulnerable to criminal abuse and subject to increased regulatory scrutiny:



- Unregistered money services businesses
- Banking of Mexican drug money
- Transfers of money through Iran
- Bribery and corruption
- Human smuggling and trafficking

Further, the recent enforcement actions have identified these common themes of deficiencies in financial institutions' Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) compliance programs to include: inadequate risk assessment processes to identify, manage and control risks; failure to adequately conduct customer due diligence (CDD) and enhanced due diligence (EDD) processes to assess and monitor client relationships, resulting in a failure to identify potentially suspicious activity; and ineffective internal controls, with respect to the Office of Foreign Assets Control (OFAC) compliance.

This was evident in the discussion of the OCC enforcement actions against Citibank, HSBC, JP Morgan Chase and TCF National Bank. In addition to the common themes mentioned above, other common characteristics and root causes for the OCC enforcement actions are:

- High-profile cases involving intense media and congressional interest
- Tend to involve large dollar amounts and multiple agencies
- Potential for criminal liability
- Failure to make BSA compliance a high priority
- Failure to establish a strong compliance culture throughout the organization
- Viewing BSA compliance as a static exercise
- Treating compliance as a cost center
- Subordinating compliance to the business line

The panel emphasized that the purpose of a risk assessment is to test the effectiveness of a bank's risk-based AML internal controls, and allows for the bank to understand its risk exposure and to tailor the risk mitigation processes to its risk profile. Key risk areas to focus on include products and services, customer types, entity types and geographic locations. The risk assessment process should identify the inherent risk across all activities and product categories across all business lines; mitigate inherent risk with internal controls, such as with policies and procedures; and understand the residual risks within the institution to be able to allocate the appropriate guidance and resources to transaction monitoring. In addition, the BSA compliance program should be risk-based to focus on higher risk areas and identify suspicious activity to include: higher-risk customers who may pose a reputational risk to the bank, higher risk products and services and geographic locations known for illicit activities. A prerequisite to attaining a meaningful assessment of risk within an international financial institution is having accurate and current customer information.

Also addressed were steps to ensure an effective CDD program exists to assess the risks and expected activity of a customer:

- CDD information should include a customer's relationship across all lines of business within the bank, including all bank subsidiaries or affiliates in all regions and countries, to permit customer transactions to be monitored and evaluated in aggregate
- The CDD process should be applied to all customers, including all bank subsidiaries or affiliates, to mitigate concealment of suspicious activity occurring through such affiliates
- A periodic review process should be implemented to determine whether due diligence information is current and the customer risk rating is accurate, based on the customer's risk

The lessons learned to effectively mitigate money laundering risk and avoid issues discussed by the panel included:

- **Emphasize BSA/AML compliance with all employees** – establishing a strong compliance culture should be set by senior management. Setting the right "tone at the top" should emphasize that compliance with BSA/AML and OFAC laws and guidelines are important and are a priority throughout the organization. This is supported by having strong policies and procedures, adequate training programs, open communication with regulators, examiners and law enforcement, both domestically and internationally, understanding whether the type of compliance program is centralized or decentralized and the applicable laws and jurisdictions in which the financial institution operates, and aligning incentives with good compliance behavior.
- **Establish and maintain internal controls regarding OFAC filters** – internal controls should be in place to prevent the circumvention of OFAC filters and there is an established system of checks and balance for individuals with authority to make adjustments to OFAC filtering software.
- **Manage AML and OFAC alerts effectively** – all transactions should be filtered through the transaction monitoring software. All alerts should be thoroughly researched to identify true matches and false positives, results should be documented and retained to ensure a proper audit trail.
- **Test the compliance program** – independent testing, internally or externally, should be performed regularly and thoroughly. Identified deficiencies should be documented and remediated promptly.
- **Prevent falsifying and stripping of transactional data** – internal controls and procedures should be implemented requiring employees to maintain accurate transactional data regarding parties involved in transactions and payment instructions.
- **Watch for red flags** – review examiner criticisms, violations of law, Matters Requiring Attention (MRA), and prior audit findings. Determine whether the BSA/AML program is not self-sustaining. Review SAR filing patterns.
- **Correct problems promptly and permanently** – develop an action plan identifying the risk, the root cause of the breakdown and resolution that is reasonable, and has concrete milestones. Devote sufficient resources and work together with examiners.

General session: Meet the U.S. regulators

This year's presentation featured panelists from the FDIC, FinCEN, OCC, Federal Reserve Bank, SEC, FINRA and the Florida Office of Financial Regulation (OFR). Each presenter provided comments regarding recent developments within their respective agencies and the financial institutions they regulate.

The panelist representing the FDIC opened by stating that increasing attention is being paid to new products and services and the involvement of Compliance in business decisions to launch these products. The launch of a new product or service should involve BSA/AML compliance from the outset. Training for new products and services should be provided to all applicable employees, including Compliance. It is also critical that policies, procedures and risk assessments are updated and approved by the board of directors. The Compliance function should also perform periodic assessments to fine-tune controls and reach out to regulators with questions or to discuss any areas of concern. Compliance involvement in mergers and acquisitions is also critical, and BSA/AML considerations should be included in strategic plans to ensure that the IT systems, staff resources and training for new employees are adequate.

The FinCEN representative discussed the database modernization initiative and the on-boarding of 8,000 users into the system for the new SAR and CTR forms after April 1. They expect a learning curve with the

new forms, and will be discussing issues as they arise with the banking industry. The panelist also discussed upcoming rules and guidance. The advance notice of proposed rule-making for customer due diligence and beneficial ownership is moving forward, and a notice of proposed rule-making will be issued in the near future. There are also upcoming notices of proposed rule-making addressing AML requirements for government-sponsored enterprises (GSE), such as Fannie Mae; declaration of prepaid products at U.S. borders; AML rules for investment advisors; and on reporting cross-border wires. FinCEN will also be releasing guidance related to e-currency, armored car transactions and clarification on previously issued guidance on foreign-located money service businesses.

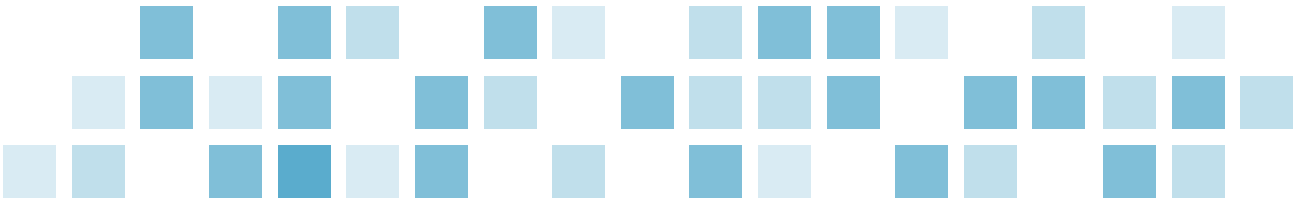
The OCC representative advised the audience to ensure that management does not over-commit during examinations with unrealistic timetables or overly comprehensive scope. Management should work on exam management by having meetings up front to explain the institution and compliance program and have weekly meetings to follow up on status. Furthermore, the panelist stated that it is OK to disagree with examiners, and encouraged the audience to stick to facts and minimize emotional responses. Management should use the exit meeting to find out the examination conclusions. If management commits to an action, it will be expected; therefore, talk to the examiners and set realistic goals, explain the disagreements and work through the facts to agree on the risks of the observations.

The panelist representing the Federal Reserve Bank recommended that corrective action plans are realistic and achievable, because the regulator will hold management to those. The panelist also noted that in foreign banking operations, the local office may be making a determined effort to address examination findings and enforcement actions; however, there is not always adequate support and attention from the head office. Often, the head office may show a lack of knowledge of regulations and not appreciate the severity of examination findings. Regulators are also increasingly focusing on senior level accountability for AML compliance, ensuring that global AML programs adequately cover the entire organization, and that foreign correspondent bank due diligence is comprehensive, including a risk assessment, and addresses affiliate correspondent banks.

The SEC representative discussed some of the key issues found in examinations of broker dealers. The SEC has found a number of instances where foreign parties have been able to access the securities markets with little or no due diligence or established controls. Issues have included little or no transaction monitoring; reliance on information provided by the party committing fraud without independent vetting; ignoring regulator comments and concerns regarding suspicious activity; failure to file SARs and lack of adequate customer due diligence on their customer's customers.

The FINRA representative discussed current trends in broker dealer examinations. In 2012, there were 1,200 examinations of members using a risk-based approach. One area of recent focus has been on the point of sale by targeting specific branch offices to focus on AML compliance. The most frequent finding is inadequate independent testing, commonly due to a lack of independence or insufficient scope. FINRA is also continuing its efforts to field a highly trained team of AML investigators to further improve coverage of AML compliance for FINRA members.

The Florida OFR representative detailed the recently implemented requirements for Florida banks regarding Iran. Banks are now required to annually certify that they are complying with the regulation and that they do not maintain accounts for the government of Iran, foreign terrorists and financial sanctions.



Beneficial ownership: Will a risk-based approach survive?

The FinCEN-proposed rule-making on beneficial ownership and the recent revisions to the FATF Recommendations portend potentially major changes in customer due diligence requirements in the near future. The panel addressed current requirements and best practices, and how their respective institutions are leveraging existing practices to address the anticipated changes in due diligence requirements. The panel included representatives from government, banking and law.

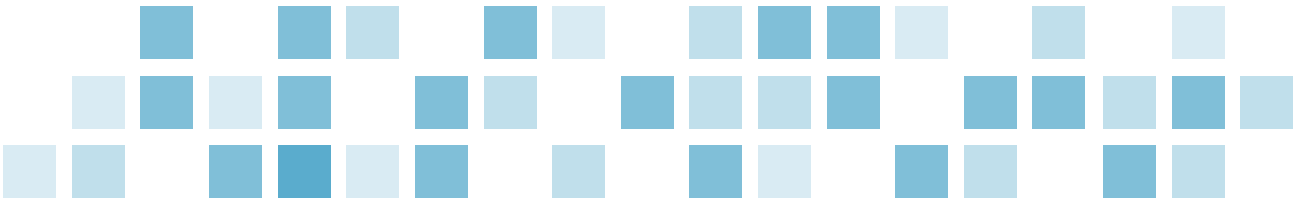
Current BSA requirements and guidance are not prescriptive with regards to information collected on beneficial owners. Financial institutions are required to have a risk-based AML program, collect CIP information for customers and account signers, and provide adequate suspect information when filing a SAR. USA Patriot Act Section 312 requires enhanced due diligence for foreign correspondent banking and private banking customers, including identification of beneficial and nominal owners. In addition, guidance provided in the form of the FFIEC BSA/AML Examination Manual, the March 2010 FinCEN Beneficial Ownership Guidance and the May 2006 FinCEN Omnibus Account Guidance mandates appropriate risk-based policies and procedures without specifying minimum requirements. This has resulted in inconsistent approaches by both regulators and industry.

Financial institutions use a variety of approaches when developing CDD procedures. For example, due diligence controls may be preventive (performed up front) or detective (performed after opening); some due diligence procedures may apply across the board to all customers and other procedures may be risk-based; the type of information collected and extent of verification; and the frequency and extent of updates to customer information can vary widely among institutions.

Two panelists shared their approaches to customer due diligence. The first panelist, from a domestic mid-sized bank, explained that one of the primary goals of the CDD process was to obtain information that is usable, particularly for screening for PEPs and negative news, and that would be useful to identify and report suspicious activity. Beneficial ownership information is collected for all customers using an ownership threshold of 25 percent. CIP information is obtained for beneficial owners, but is not validated or verified, and risk points for the beneficial owner, i.e., for being a PEP, are applied to the overall customer risk score. EDD is triggered by the customer risk score, which is primarily driven by actual activity. The biggest CDD-related challenge at this institution is backfilling and refreshing information for existing customers.

The second panelist, from a bank with significant presence in the U.S. and Canada, uses a tiered approach to CDD. Identification of beneficial owners controlling 25 percent or more is required by Canadian regulations for all customers with no requirement for verification of information, and the bank requires identification of owners controlling 10 percent or more for higher-risk customers. Risk factors for beneficial owners are incorporated into the overall customer risk score. Customer risk rating is performed post-hoc and includes risk factors for geography, products/services and actual activity. Updates to customer information are event-driven, such as an existing customer opening a new account. Highest and high risk-rated customers are refreshed semi-annually and annually, respectively. Canadian regulations require refreshing CIP and CDD information every two years. The bank uses the same standards for its retail banking and broker/dealer operations. Some significant challenges include obtaining all required information at account openings, providing adequate training of frontline retail staff and linking accounts with common ownership.

The next panelist provided perspective from the securities industry. Broker/dealers have always collected customer information, including sometimes on beneficial owners, to determine suitability for investments.



Currently identification of beneficial owners controlling 10 to 25 percent is common for high-risk accounts. FinCEN's March 2010 guidance led to confusion in the securities industry over requirements related to verification of beneficial ownership and the application of EDD procedures. In response, the Securities Industry and Financial Markets Association (SIFMA) release a white paper to help clarify the guidance. In response, subsidiaries of bank holding companies, where pressed to adopt global compliance programs, redoubled efforts to verify the adequacy of existing systems for documentation and monitoring. The panelist also noted that for the most part, beneficial ownership is not verified, except when dealing with PICs, and customer information is generally not updated.

Attendees heard an overview of the government's approach to the proposed beneficial ownership rules. The goal of the rules will be to maintain a risk-based approach to due diligence, and level the playing field between institutions that exert significant time and resources to identify beneficial owners and those that do not. The issues raised through the industry town hall meetings and comment process are being considered and will hopefully be adequately addressed by the proposed rule. The panelist stressed that the goal is to establish a framework that leverages existing practices in the industry, and not be overly prescriptive.

Key elements of the CDD program envisioned by the proposed rules include: initial CDD at account opening, including CIP; understanding the purpose and intended nature of the account, the expected type and volume of activity; identifying beneficial owners and risk-based verification; and ongoing risk- and/or event-based monitoring and updating of CDD information. Existing exemptions to CIP will likely apply to the new rules and there may be additional exemptions. Other issues being considered include extending CIP reliance to CDD, and whether FIs will be able to rely on customer certifications.

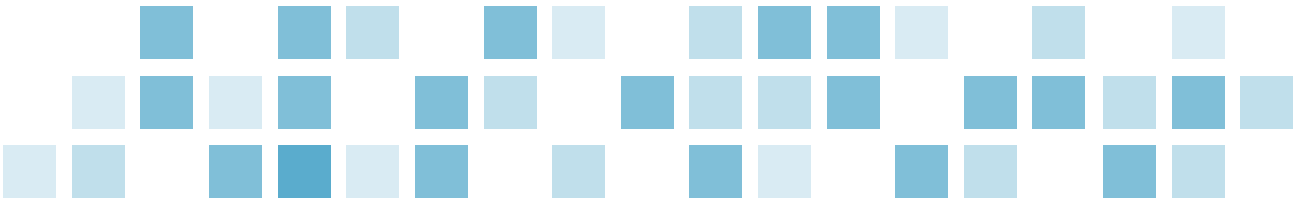
The definition of beneficial ownership in the proposed rule has two prongs:

- Individuals directly or indirectly owning more than 25 percent of an entity, or if no one satisfies that definition, the person with at least as much ownership of the entity as any other individual
- The individual with greater responsibility than any other for managing or directing the entity's regular affairs. The rule considers a beneficial owner to be a natural person.

The government has been soliciting industry comments to determine if this definition is understandable and practical. The level of verification is also being debated. Does verification mean confirming the identity of the beneficial owner or confirming the individual is a beneficial owner of the entity in question? The government will also have to determine how to reconcile the proposed 25 percent threshold with the 10 percent threshold in the FATF Recommendations; and decide how CDD will be applied to intermediated accounts, such as omnibus accounts, customers acting as agents and trusts.

Evolving Caribbean regulatory environment

This session discussed how Caribbean nations are preparing for the fourth round of Caribbean Financial Action Task Force (CFATF) Mutual Evaluations; whether the number of money laundering (ML)/financing of terrorism (FT) prosecutions have increased; and the status of national threat assessments as a result of regulatory and supervisory efforts. The panel included speakers from the regulatory, law enforcement and industry perspectives, representing St. Kitts-Nevis, St. Vincent and the Grenadines, Belize, the Cayman Islands, Jamaica and the Bahamas.



Bahamas

The Bahamian economy is sustained primarily by tourism and international financial services. Financial services constitute the second most important sector of the Bahamian economy and account for about 20 percent of the Gross Domestic Product (GDP). Since 2000, the Bahamas' compliance with international AML/CLT standards are reflected in the ratification of new and enhancements to domestic legislation. In 2001, the Bahamas was removed from the FATF's Non-Cooperating Countries and Territories (NCCT) list. The panel speaker discussed the efforts of the Bahamas to restructure its financial services regulatory framework, with particular emphasis on Designated Non-Financial Businesses or Professions (DNFBPs). The third round of Mutual Evaluations revealed areas for improvement and lessons learned, and provides the context for which preparation of the fourth round of Mutual Evaluations will include strategic planning, legislative review and effective implementation of revised recommendations.

Belize

Belize is bordered by Mexico to the north and Guatemala to the south and west; therefore, it is a country that is vulnerable to money laundering activities. The panel speaker discussed that the most recent Mutual Evaluation, based on information obtained in April 2010, cited several weakness with AML/CFT regime. Recommendations are being implemented that include action plans and timelines for completion, and several legislations are being amended to become compliant with FATF 40+9 Recommendations to prepare the fourth round of Mutual Evaluations. The panel speaker highlighted some of the key efforts of the Financial Intelligence Unit (FIU) to include: initiating a registration process for DNFBPs with a Supervisory Authority; establishing regulations and guidelines relating to DNFBPs; training and education of DNFBPs to be become more compliant with the Money Laundering Terrorism Prevention Act; modeling FIU regulations and guidelines after other FIU's; and increasing collaboration and cooperation with other Supervisory Authorities.

Cayman Islands

The panel speaker noted that economy of the Cayman Islands is similar to that of the Bahamas, and faces some of the same challenges to ensure compliance with FAFT 40+9 Recommendations. The panel speaker discussed the efforts of the Cayman Islands to prepare for the fourth round of Mutual Evaluations to include: finalizing the implementation of the third-round recommendations; implementing the new FAFT 40 Recommendations; demonstrating the effectiveness of the action plans; increasing collaboration and cooperation across agencies; and understanding the resource challenges and impact on financial institutions.

Jamaica

The panel speaker addressed both FATF issues and non-FATF issues during the presentation. The FAFT issues include: addressing DNFBPs, non-regulated financial institutions, charities and arrangements for legal persons; developing National Risk Assessment(s) with appropriate controls associated and mechanisms to capture data to show the effectiveness of the controls implemented; introducing amendments to legislation to capture the changes with FAFT 40+9 Recommendations; and keeping abreast of the new evaluation methodology, as Jamaica is one of the first countries to be evaluated. The non-FATF issues included: reforms to improve growth prospects; development of approaches and legislation for financial inclusion; enhancements to the deposit-taking sector laws and amendments within the Omnibus legislation to address the financial stability issues; and the challenges to ensure compliance with Global Forum, Financial Sector Assessment Program and Foreign Account Tax Compliance Act requirements.

St. Kitts-Nevis

The panel speaker highlighted the challenges and changes as a result of the third-round Mutual Evaluation. Three key challenges were discussed: the enactment and amendment of laws due to changes in the

parliament and the parliamentary timetables; AML training with limited funds and availability of training locations; and staff recruitment and turnover. The changes made included: defining the AML/CFT operational chain, roles and functions; increasing staff with trained personnel; increasing onsite inspections and educating businesses and consumers of the AML/CFT programs; having a fully functional ML investigative unit; and introducing laws and legislation that are specific and timely and sanctions that are proportionate. In order to prepare for the fourth round, St. Kitts-Nevis is keeping abreast of the FATF's new evaluation methodology and standards, and enhancing efforts around AML effectiveness through increased communication, human resources and AML skills.

St. Vincent and the Grenadines

The panel speaker addressed the regulatory environment of St. Vincent and the Grenadines. Prior to 2001, the Proceeds of Crime Act, No. 12 of 1997, provided the regulatory guidance related to the prevention of money laundering and any other related matters. After 2001, St. Vincent and the Grenadines enacted legislation, and created the National Anti-Money Laundering Committee and Financial Intelligence Unit to establish the necessary infrastructure to ensure it has a strong AML/CFT program. The panel speaker addressed recent development and updates. There are amendments and proposed amendments to the current legislation, and the case of Andrews et al v. Attorney General of Saint Vincent and the Grenadines HCVAP 2010/019 was upheld on appeal and is pending additional review by a higher court. The panel speaker discussed the prosecutions, cash seizures and forfeitures relating to money laundering activities, and the efforts to increase AML/CFT training and awareness through government publications and SAR analysis.

Broker dealer and wealth management round table

The round table was open to questions from the audience. The panel included speakers from the SEC, FINRA and industry. The discussion was focused on issues such as unregistered broker dealers and market manipulation schemes.

Popular schemes discussed by the panelists during the session included low interest rate products and master/sub account arrangements. Low interest rate products are structured products for which the broker dealer fails to disclose the true risk associated to the highly risky product. These are real products that are not fully explained to the public. In NASD Rule 1018, FINRA states that for firms that maintain master/sub-account arrangements, depending on the facts and circumstances of such arrangements, a firm may be required to recognize the sub-accounts as separate customer accounts for the purposes of applying FINRA rules, the federal securities laws and other applicable federal laws. A red flag is when the entity has a high volume of day trades through the accounts and takes the orders from the sub-accounts. The firm is responsible for monitoring their own suspicious activity, and market manipulation is a suspicious activity category included on the SAR Form.

The presentation followed with questions from the audience. One question addressed registration requirements for foreign finders or referral agents. Foreign finders are required to be registered. The risk comes in when there is no record of an entity to have searched and verified that the foreign finder is registered. NASD Rule 1060(b), is a safe harbor that provides exemptions from the Rule 1031 requirement related to the registration of persons associated with a member who is engaged in the investment banking or securities business. NASD Rule 1060 provides exemptions from that requirement. NASD Rule 1060(b) states that members and persons associated with members may pay to non-registered foreign persons transaction-related compensation based upon the business of customers they direct to member firms, if certain conditions are met. This rule provides members with assurance that they may pay foreign finders under the circumstances

described in the rule and not have to register those foreign finders as associated persons. NASD Rule 1060(b) was intended to provide this assurance in situations where the sole involvement of the foreign person receiving the transaction-related compensation is the initial referral of non-U.S. customers to the member. Policies and procedures around this rule should be in place. The entity should be able to monitor the foreign finders. The risk comes in when the foreign finders start acting as relationship managers, and even have access to the trading accounts.

Another question addressed the risks associated with foreign currency transactions with Venezuela Bonds. Dealing with deposits of security into the U.S. broker dealer can create a variety of issues. The fact that 80 percent of the U.S. broker dealers' revenue comes from Venezuela is of great concern. There is often little to no due diligence being performed on these customers, and U.S. brokerage firms are jumping into the business without a proper AML/BSA program and with little to no experience in the matter. The firms need to understand their clientele. Set-me-up transactions are risky transactions related to countries with currency restrictions, like Venezuela. These are transactions for currency exchange, and not for investments purposes. The firms must have controls in place to identify these types of transactions.

An audience member asked if Argentina was a jurisdiction of concern. The panel response was that any country with currency control is of concern; for example, Venezuela, Costa Rica, Colombia, Panama, Guatemala and Argentina. Registered investment advisors should have an AML program in place that will allow the monitoring of transactions related to these countries.

Panelists also addressed independent testing. When hiring an outside firm to conduct the testing, it is important to interview the firm. Ask questions to others that have used the firm and ensure that it is knowledgeable in the area. Ensure that sufficient testing is being performed and that all high-risk areas are covered.

As a final recommendation, one of the panelists noted that it is important for the broker dealer to have an enterprise risk assessment and an internal control review. Setting meetings with Senior Management regularly is critical. This allows for the better understanding of internal systems and control, and to assess risk. It is essential to understand that compliance issues are not just a problem of the Compliance Department.

Meet the enforcers: The financial crime prosecutors

This session provided the attendees the opportunity to understand U.S. financial crime enforcement efforts. The panel represented state and federal prosecutors and investigators. Panelists discussed the differences between criminal vs. regulatory enforcement, state vs. federal enforcement, the issues arising from multiple jurisdictions, and the challenges with investigating the same conduct, both domestically and internationally. Because many investigations begin with Suspicious Activity Reports (SARs) to identify trends and red flags for specific behavior, the panel emphasized the importance that financial institutions develop relationships with law enforcement and regulators. SARs should provide information that is detailed and specific to the nature of the suspicious activity. Panelists also explained that the reported dollar amount does not attract the attention of the investigator as much as the trend of the activity. Furthermore, only 1.5 percent of SARs are of interest to law enforcement, and result in additional investigations and prosecution.

Efforts have been increased to identify financial crimes through the creation of SAR review teams and financial task forces with the U.S. system. The panel explained that the purpose of this effort is to be more proactive and focus on other areas of concerns, such as identity theft and terrorist financing.

Panelists discussed the impact whistleblower incentives have on the investigation of financial crimes. The panel noted that there are several U.S. agencies that have whistleblower incentive programs, and the amount of the award is a percentage of the amount collected or seized if information is used. Panelists emphasized that although whistleblowers are useful and helpful in cases and are encouraged to come forward with information, they are not a substitute for investigations to prove financial fraud and conduct.

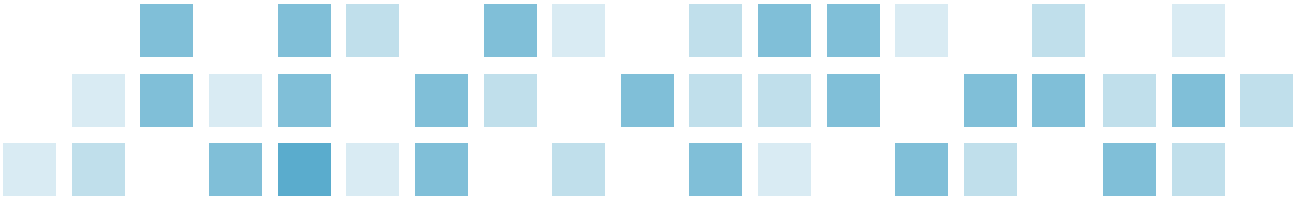
The panel presented the following cases against HSBC, Wachovia and MoneyGram, in which there were apparent breakdowns within the Anti-Money Laundering and Bank Secrecy Act programs, leading to the involvement of criminal prosecutions. The common theme in each of these cases was the inability to detect fraud and the lack of corporate accountability. A question was posed as to why more criminal cases are not brought against individual persons involved in corporate breakdowns of regulatory compliance. The panel stated that there is difficultly in pursuing those types of cases because they are difficult to prove. Panelists reemphasized the need to have strong and effective compliance programs within your organization.

FCPA and anti-corruption

This presentation focused on recent FCPA cases and best practices for building an anti-corruption program. The panel began by expressing the need for the preclearance of expenses related to the entertainment of foreign officials. The sources of funds at account opening by most institutions has an FCPA competent to it, since adequately identifying the source of funds may be able to determine if funds are potentially illicit. Institutions face the risk of employees engaging in corruption while acquiring new clients. One panelist questioned that if it is "raining corruption" in one area, if it is even worth the risk for the institution to conduct business in that area.

Next, the panel discussed the 2012 Latin America Corruption Survey. The results of this survey indicated that half of all respondents believe their company has lost business to competitors making bribes in the region, and only 28 percent of respondents believed anti-corruption laws are effective in the country where they work. Chile (78 percent) and the US (70 percent) are seen as having the most effective laws. Corruption was seen to be a significant obstacle to doing business in the region by 44 percent of respondents. The most significant corruption challenges were reported to be Venezuela, Argentina, Mexico and Bolivia, and the lowest levels of corruption were reported to be Chile, Uruguay and the U.S. Corruption risks differ by countries. Corruption risk in Mexico was most associated with policy and municipal/local governments, risk in Argentina was associated with the executive branch of government and customs, and risk in Brazil was most associated with the legislative branch, police, municipal and local governments and customs. The study also found there was an increase in the attention multi-national corporations are giving to compliance with the FCPA.

The next topic focused on the challenges faced by Siemens following a bribery scandal. Siemens was subject to over $2 billion in files and legal fees, as well as extensive reputational harm. The entire telecommunications group was terminated as a result of their role in the bribery scandal. Siemens now spends over 100 million euros a year on their compliance program. The program has since been enhanced to add an investigation unit. Currently, investigation units are located in Mexico, Brazil and the U.S.; however, the units are relocated as necessary. It is possible for institutions to recover from such scandals; Siemens has had their two most successful years ever since the scandal occurred. Also as a result of the scandal, Siemens is subject to extreme regulatory scrutiny. Every aspect of the compliance program is scrutinized on a daily basis. The World Bank, as well as the U.S. Department of Justice, maintains a dim view of Siemens. The institution must remain vigilant to all compliance risks, and Siemens has been informed that any future problems with U.S. regulators will result in the institution being delisted from NASDAQ, which will have a far-reaching impact on the institution's business



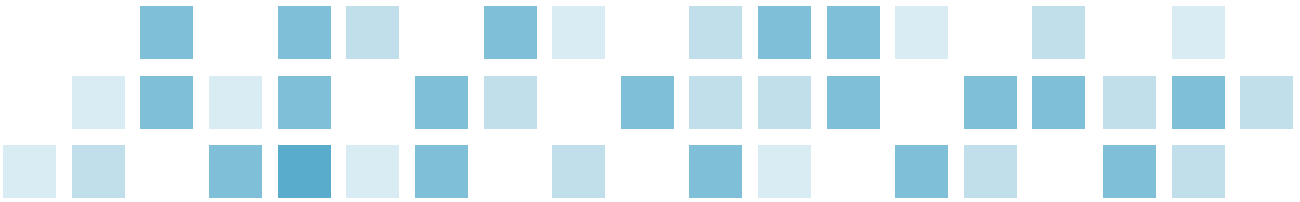
worldwide. He cautioned institutions using recruiters who guarantee access to clients must be handled with extreme care by institutions, since individuals like this carry enhanced risks to the institution.

The next panelist began by stating 10 percent of the workforce will never engage in an illegal act, no matter how easy, and 10 percent will always try, no matter how hard. The challenge is to manage the remaining 80 percent to protect the institution. Banks face business pressures, which may result in employees circumventing controls. The tone at the top is vital to an organization. Rational behavior must be emphasized. Senior management must have access to the board to report significant issues. Institutions must maintain a zero tolerance for bribery. It is also in institutions' best interest to encourage employees to come forward. Whistleblower programs allow employees to go straight to the SEC and potentially earn up to 20 percent of future penalties. Baseline training must be made to all employees, with supplemental training for employees more exposed to potential FCPA activities. It is not sufficient to provide training to employees; institutions must measure the success of the training. Results should be analyzed to identify areas of weakness (identify questions answered incorrectly). Gaps in knowledge should be addressed immediately. Case studies of ethical dilemmas should be included for the most vulnerable employees. These studies should address the following questions:

- Is this action the right thing for the bank?
- Is it consistent with the bank's practices?
- Is it legal?
- Can I be accountable for it?

Third-party providers, such as recruiters or finders, also pose additional risk. Liability for the actions of these providers flows to the institution, not the recruiter. This risk can be mitigated through effective due diligence completed by the institution prior to utilizing the recruiter. If the institution does not do proper due diligence prior to engaging the recruiter, it is assumed the institution turned a willful blind eye to the possibility of the recruiter engaging in illegal activity. If an institution is considering a joint venture with another business (e.g., construction, private equity transactions, etc), due diligence should include a corruption-specific component. The Bank will be held responsible for the actions of the partner firm; therefore, due diligence must be consistent with the Bank's policy and be well-documented. For any potential ventures, all parties must be verified against government lists and legal databases, and general Internet searches should be performed. Contracts should expressly state the controls around the relationship. The institution should consider sending a team in to review the other business's AML program and/or to train the other business as to how the institution's compliance program works. This should be viewed as a good opportunity to sell the compliance program to the other company as an added value in the venture. EDD should be performed of course, including the business climate in the region, any sovereign families which may be involved in the business to review for the potential comingling of funds, the history of the firm and the nature of the business. A business with a limited history or a change in the type of business should be considered red flags.

Certain regions, including China, will pose additional risks where gift-giving is an ingrained part of the business culture. For institutions operating in such regions, there is a need to comprehend the rules around the region, as well as a firm understanding of the institution's policies. There should be strong segregation of duties surrounding gift-giving. All gifts should be pre-cleared and approved by someone outside the business unit. Parameters such as monetary limits for gifts should be well-defined. Gifts must also be monitored in terms of the frequency of gift-giving, the amount of gifts and who is receiving the gifts. The institution must ensure gifts are spread out and not repeatedly given to the same individual, and should also ensure numerous gifts are not given to businesses located at the same address.



Entertainment of government officials may be a necessity, but the institution must review the risk involved, ensure that front-end people truly understand the risk of their actions, and pre-clear all expenses related to the entertaining of foreign government officials. Gifts must be monitored and questions asked for anything that doesn't make sense; i.e.," why did we spend $3 million in Mongolia?" Contracts with venture firms should include general items, such as termination clauses, specifically address FCPA, clear language discussing improper payments, as well as more specific language concerning the local language, local landscape and audit rights. Audit rights have different meanings in different countries. Some countries would only require periodic financial audits; others may include internal audits. Caution should also be taken when contracts are translated, as translations may be awkward and phrases may lose their intended meaning. Local attorneys should always be consulted with.

Institutions engaging in foreign correspondent banking should understand the nature of the customer's business and maintain a heightened awareness of the risks associated with the region the correspondent bank operates in. Small periodic look backs should be performed to verify the transactions occurring in the account.

A discussion of the difference between lobbying and corruption concluded the session. Corruption is present in every country; however, there is a difference in FCPA-prohibited activities and lobbying. The difference is defined by government regulations. Contributions to political parties and candidates are, of course, legal, while payments to foreign officials to gain improper advantages are illegal. Corruption can be viewed as an unauthorized benefit to make a transaction on your behalf. Institutions should be mindful of individuals seeking payments to enrich themselves and consultant fees should be reviewed for reasonableness. Finally, organizations should monitor and document the purpose of payments; the absence of information should be reviewed as a red flag.

Conclusion

McGladrey was proud to serve as a sponsor of the Florida International Bankers Association 13th Annual Anti-Money Laundering (AML) Compliance Conference.

This summary offered only highlights of the conference. It is not intended to be a complete review of all material covered.

McGladrey professionals welcomed the opportunity to learn, network and educate alongside bankers, regulators and other interested parties, and congratulate FIBA on another successful conference.

Questions about the specific topics highlighted in this summary or about other AML subject matter considerations are welcome.

800.274.3978
www.mcgladrey.com