20203 Goshen Road, No. 343 • Gaithersburg, MD 20879 USA
+1-301-330-1970 • www.doccreditworld.com • info@doccreditworld.com

Executive Summary of the 2017 ABA/ABA Financial Crimes Enforcement Conference

3-5 December 2017, National Harbor, Maryland, USA

An annual event for Anti-Money Laundering and Fraud Professionals, the 2017 conference conducted by the American Bar Association's Criminal Justice Section and the American Bankers Association attracted over 850 registrants from the banking, legal, compliance and regulatory spheres. The three-day event featured 23 concurrent sessions delving into specific issues, six general sessions taking up topics of concern to the audience at large, six "power hour" breakfast sessions and two luncheon sessions.

Sunday, 3 Dec 2017

Third Line of Defense: Assessing the Effectiveness of AML Controls – Auditors serve as the third line, a critical and necessary link between a bank's AML/compliance specialists and regulatory examiners. A poor audit report can be a wake-up call that corrective actions are needed by the second line and may trigger more resource allocation in some cases. If issues are adequately addressed, they can be remedied before examiners come in. Regarding audit approach, panelists weighed continuous vs. periodic. Each method has its challenges and advantages. For one auditor, descriptive analytics, rather than random samplings, has become a growing aspect of their audit approach. The audit function requires evaluation of testing and identification of data that can be leveraged.

International AML Hot Topics and Trade-Based Money Laundering Concerns – No longer a topic of concern solely for large international banks, all banks and businesses engaged in trade need to be cognizant of the threat. The panel referenced recent US government actions including a FinCEN advisory on how North Korea accesses the international financial system. With the bulk of trade handled on open account, wire transfers and checks/drafts are the most convenient vehicles for TBML and are difficult for banks to detect due to lack of documents to examine or trace. Diversion of items (often dual-use goods), commonly through transshipment ports, has become a huge risk for banks and legitimate trade. The panel cited examples of dual use commodities, including pressure transducers, and red flags. While not illicit, abuse of the gray market is problematic. Case studies analyzed included: Bank of Dandong; Turkish front companies; the Khanani money laundering network; and Chinese use of Bitcoin. Sanctions evasion typologies and effective clues for detecting them were examined. Not only must banks heed sanctions, they should assess the compliance of those with whom they have correspondent bank relationships and know their exporters.

General Session: Challenges and Solutions in Managing Financial Crimes Function – When dealing with financial crime, it is important to have communication and synergy within the institution. There is a worry that too much separation between the people who handle specific financial crimes, such as fraud, AML, sanctions, cyber, etc., will allow for important information to go unaddressed. It is necessary for all of the financial crime units to look at SARs. For instance, an act of fraud could also be a cyber crime and/or money laundering. Another issue is the different timeframes for filing SARs depending on the type of financial crime that has occurred. It may be important for a financial institution to therefore align its different financial crime divisions so everyone at the financial institution is on the same page. In addition to cooperation within an institution, cooperation with law enforcement is also essential as it can allow for information to be shared and can serve as an educational tool for both parties.

One issue facing financial institutions is what is a new account for purposes of doing KYC. Some institutions use the issuance of a new account number as the benchmark. Therefore, the renewal of a CD or loan would not qualify. Financial institutions must decide for themselves what policy is best to follow.

Another rising issue banks face is marijuana, as more US states legalize it for various uses. However, marijuana remains a controlled substance at the federal level and US Attorney General Sessions has hinted that he may take a more aggressive stance toward enforcement than the previous administration. Banks must decide if they want to have a relationship with customers that deal with marijuana, however, it may not always be as easy as dealing with a new business that approaches the institution. What if an existing customer comes to the institution, such as an oncology clinic that wants to grow and dispense marijuana for medicinal purposes? What about a supplier that produces equipment that can assist in the growing process? Or, what if an institution has decided not to deal with customers in the marijuana industry but a customer lies about its business? The bank may have to judge whether such behavior rises to the level of filing a SAR.

General Session: Reg Tech Impacts on Financial Crime Investigations – The use of artificial intelligence (AI) tools in banking is crucial to combatting financial crime more effectively and more efficiently. The UN has estimated that there is USD 1.5 trillion in financial crime annually and only 1% is caught. AI can be used to automate certain "yes/no" functions. Two of the most effective ways AI can be used is in transaction monitoring and in dealing with "false positive" hits, allowing employees more concentrated focus on the SARs that are actual financial crimes. AI can also be used to analyze SARs, allowing institutions to share patterns with others institutions to combat financial crime. However, this can be complicated in jurisdictions that restrict data sharing.

Other Sessions – Also held on Day 1 of the conference: Diagnosing and Dealing with Current-Day Challenges of Legacy Transaction Monitoring … From Talent Management to Governance, Operational Considerations for Community Banks … What You Should Know About [New York State Regulation] Rule 504 … The Intersection of AML, CFT, Cyber and Fraud for Mid-Size/Large Banks

Monday, 4 Dec 2017

General Session: Regulatory Enforcement Issues – The first part of this session featured a conversation with FinCEN and OFAC directors who indicated enhanced cooperation is building between the agencies and their core principles of strict liability (OFAC) and risk-based focus (FinCEN). FinCEN is attempting to step up action taken against non-banks violating AML laws. The message was also conveyed that FinCEN does not want to frighten good people away from difficult jobs. OFAC is most concerned about willful and reckless activity. Reinforcing that it encourages self-disclosures, OFAC does not want banks and non-banks to "under sell" when violations occur. OFAC also urges greater broad-based outreach and shies away from communication with individual institutions.

Part two of this session involved a panel discussion among regulatory officials. Although gross violations garner major attention when they are made public, the industry is not falling apart. Most violations are much more nuanced. With the 11 May 2018 date for mandatory compliance with the Customer Due Diligence Requirements for Financial Institutions (CDD Rule) looming, many banks are reportedly ready for it but others need to incorporate into their bank's internal controls. One specific aspect of the CDD Rule that has the attention of banks is the Beneficial Ownership aspect, particularly that banks must identify each individual who directly or indirectly owns 25% or more of the equity interests of a legal entity. One regulator cautioned that banks should take a holistic approach rather than technical interpretation of the CDD Rule. As banks develop approaches toward confronting the regulatory challenges facing them, regulatory officials are looking for good records and documentation, adherence to following their controls, transparency, and a willingness to seek guidance when necessary. Regarding matters of derisking and balancing between compliance and inclusion, regulators are asking institutions to consider customers on a case-by-case basis and devise ways of managing appropriate risk instead of eliminating all risk.

Sanctions Enforcement Trends – Banks must cope with a broad mix of general, surgical, and vague sanctions. Recent changes include comprehensive UN sanctions dealing with energy restrictions. There is now authority for secondary sanctions to be imposed on third party companies doing business with North Korea. By virtue of US OFAC's 50 Percent Rule, if a sanctioned entity owns 50% of an entity, then that entity subjected to sanctions as well. Apart from OFAC, the US State Department has its own lists. Regarding the US Executive Order applying new North Korea Sanctions, panelists discussed whether banks are responsible for monitoring vessel IMO numbers. For named vessels, banks need to. With letters of credit, there is more responsibility because LCs have more information than wire payments. As evidenced by other updates toward Russia, Iran, Cuba, and Venezuela, sanctions are constantly changing, becoming more complicated, and mere screening of lists is insufficient. In the future, one panelist predicted that banks will see much more information sharing by the government with the private sector.

Luncheon Speaker: US Treasury Under Secretary Sigal Mandelker – In her capacity leading the US Treasury's Office of Terrorism and Financial Intelligence, Under Secretary Mandelker announced launch of FinCEN Exchange, a new public-private information sharing program that FinCEN will lead. One component of FinCEN Exchange will be regular briefings with law enforcement, FinCEN, and financial institutions to foster the exchange targeted information on priority illicit finance threats. Participation is voluntary, but Mandelker believes such cooperative efforts will strengthen the AML system without placing added regulatory burden on financial institutions. The full text of Mandelker's Keynote Address is available at: https://www.treasury.gov/press-center/press-releases/Pages/sm0229.aspx

Threats and Red Flags: Emerging Fraud Risks – By one published estimate, 2%-5% of global GDP is laundered, amounting to as much as USD 2 trillion. Banks are competing against fraud as a profession and fraudsters have their own playbook. The evolution of fraud is such that illicit actors will target vulnerabilities, exploit weaknesses, apply new technology to traditional attacks of the past, and repeat what's proven successful for them and criminal peers. Banks' approaches toward counteracting fraud have been fragmented as an industry and even within institutions. There's an opportunity for collaboration and a cross-institutional approach can fortify protections against fraud. It is also imperative that banks formalize controls and share information with those that defeat the initial threat. Panelists also addressed specific trends in fraud investigative techniques.

Negative News: Verified vs. Unverified – Given the abundance of negative news and varying degrees of accurateness, how do banks filter for and use relevant adverse information? Panelists discussed how banks apply negative news toward their risk assessments. Is a conviction proof-positive of a reputational risk and does it matter whether or not it is a financial crime? How are allegations evaluated? At the international level, there are differences and additional considerations. An institution's response to negative news has to be multifaceted. In considering negative news, banks must determine if it impacts a core or non-core activity of their institution. Confronted by regulators with negative news, banks will be expected to be honest from the outset. Banks need to ensure they have designed and implemented an approach toward handling negative news impacting customers, counterparties, and their own reputation.

General Session: The Dark Web and More: Monitoring and Detecting Cyber-Enabled Crimes – Reputable professionals with expertise of this realm briefed the audience on how the dark web is used to target individuals and institutions. A subset of the deep web, the dark web is primarily used for illicit purposes and to conceal. The well-intentioned should not casually venture into or experiment with this space. Access to the dark web is vigilantly controlled and built on trust among criminal elements. The dark web has a forum for communication and marketplace for advertising goods and services. Bad actors operating on the dark web all have areas of specialty, including the design and distribution of malware. A team effort is essential for combating it. The technology and fraud prevention sides within banks need to work together. Auditors need to know what the threats are before they happen and technology specialists need the right cyber skillsets.

Other Sessions – Also offered during the conference: Strategies to Deal with False Positives … The Future of AI in Financial Crimes … Best Practices and Benchmarking for Your AML Program … New Payment AML Threats … A Tactical Approach to CDD/Beneficial Ownership for Banks for Mid-Size/Large Banks (separate session for Community Banks) … Data Quality … Model Governance for Mid-Size/Large Banks (separate session for Community Banks) … Banking Marijuana Businesses … Key Risk Indicators and Other Metrics for Senior Management and the Board of Mid-Size/Large Banks (separate session for Community Banks) … AML and Tax … New Product AML Risk Assessment … Derisking Impact for Community and Mid-Size Banks.

Tuesday, 5 Dec 2017

Rising Regulatory Expectations for the Scope and Documentation of Independent Testing – To adequately address heightened regulatory expectations, auditors need to take charge of the independent testing process. Third party auditors have to challenge the risk assessment findings of a bank's second line of defense, although they can leverage the results. Auditors need to determine if detection mechanisms are catching the right things and the effectiveness of a bank's investigative procedures. Auditors also need to review a bank's model validation outputs, sampling, test scripts, and controls. If changes are made to testing parameters, the reasons must be documented because examiners will ask auditors why changes were done.

General Session: The Legal Implications of Recent Fraud and Money Laundering Cases – A panel of legal specialists took up discussion of five cases which offer relevant lessons for bankers and regulators. The first case involved a political

individual who had secured a loan and maintained foreign bank accounts, but failed to indicate on tax documents that he had such foreign accounts. Should such an individual be considered a Politically Exposed Person (PEP) and should banks ask for their tax returns? Another case involving a hardware store which sold massive amounts of a product used for illegal drug manufacturing presented a scenario that could be adapted to money laundering cases. When funds are confiscated, what amount is a bank "on the hook for" and what portion did it make as a profit? A third case involved a lawyer/politician providing case referrals to law firms. When illicit funds were deposited and comingled with clean funds, should that have sparked red flags from the bank? Even under additional scrutiny, perhaps not but political figures can pose challenges for banks. Another case involving litigation in two jurisdictions regarding alleged LIBOR manipulation spawned the question: Can non-US investigators take away a US citizen's right of protection from self-incrimination? The case signals a burden for the US government to prove it got information on its own accord and independent from foreign authorities. A fifth case involved misfiling of a whistleblower complaint under the US Sarbanes-Oxley Act instead of the Dodd Frank Act. As a result of different reporting requirements, the whistleblower lost protections.

Derisking Impact for Community and Mid-Size Banks – As larger banks derisk, certain business opportunities are flowing to smaller banks. Four speakers from significantly different regions of the US offered insights on how community and mid-size banks evaluate whether to bank or not bank high risk customers. A recent trend is that regulators want to see a bank's risk appetite statement approved by its board because it creates added accountability. Speakers commented on how they determine their preferred customer types, those prohibited, and others requiring special approval. For banks at this level, not all branches can take foreign nationals as customers. What bank products are desired (savings account, big business checking account, LCs) makes a difference as well. Some banks conduct initial and/or followup site visits. For high risk customers, banks will charge more and ask for additional documentation. To gain the confidence of regulators that they are capable of managing risk, community and mid-size banks must build credibility on the surface and back it up by demonstrating they have proper governance and controls in place.

Luncheon Session: Conduct Culture Considerations for the Financial Crimes Community – There is no statutory definition of "conduct culture" for US banks. At present, regulators seem willing to allow banks to define it but the industry senses it has a limited window of time to figure it out for themselves. For instance, Europe is considerably ahead in this space. While some US bankers focusing in this area say that culture can be measured, the greater challenge they believe is determining how culture impacts conduct. The assumption that misconduct is due to bad culture is not always true. Although the best conduct culture program will not be free of jerks, criminals, and greedy bankers, the concept should encompass the setting of ethical parameters for bankers akin to what exists for doctors, lawyers, and certain other professions.

General Session: Reimagining BSA/AML Compliance – The Bank Secrecy Act has been in existence nearly 50 years and every change since 1970 has been an additive. There is widespread belief, even among government regulators, that the system is not functioning properly and needs revamped. According to speakers in this closing session, now is the right time for contemplating a more efficient and effective system. If implemented properly, FinCEN Exchange could be a useful initial step. Greater focus needs placed on data as well as counteracting derisking which some speakers say is a consequence of a system gone awry. There was also a call for cooperation among those responsible for US Code Title 12 (Banks and Banking) and Title 18 (Crimes and Criminal Procedure). Other speakers suggested striving for more convergence, greater financial inclusion, and increased sharing of timely information with law enforcement.

Other Sessions – Also held on Day 3: The AML of Tomorrow and Next Generation Screening … Combatting Human Trafficking … Merger & Acquisition AML Due Diligence Hot Topics.