

Overview of the Application of Technology to
Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)
Compliance Programs

2003-2004

The world of international financial services regulation is changing rapidly and so is the increasing “cost of business” for every Financial Services Provider (FSP). Ensuring compliance with all relevant regulations requires every FSP to review its strategy and improve its business practices. Financial Services Providers around the world are increasingly recognizing the importance of ensuring that their institutions have adequate policies, procedures, systems and controls in place so that they are not used for criminal or fraudulent purposes. These systems and controls are often required by the various regulators around the world. Without such compliance safeguards, FSPs can become subject to reputational, operational, concentration and legal risks which can result in significant financial costs. Moreover, taking a positive approach to regulation can improve performance, enhance profitability, accelerate growth and build competitive advantage.

The key to the prevention and detection of money laundering and the combating the financing of terrorism is an effective compliance program. An effective compliance program should, at a minimum, consist of the following key elements: policies, procedures and controls, customer identification and due diligence, monitoring, reporting, training, and record keeping. Integrating technology can be particularly useful in the areas of customer identification and due diligence, monitoring, reporting, training, and record keeping.

There is no doubt that the financial and administrative burden of regulatory compliance is increasing daily and can be devastating. For many large FSPs, the application of technology to the compliance process may very well be the only means to meet their compliance obligations effectively. Technology is fast becoming a viable solution in almost every aspect of compliance and it allows FSPs to focus on their core competencies. In some cases, the application of technology may well result in a greater degree of compliance than those FSPs operating without it. It is interesting to note that a stunning 92% of compliance professionals, who participated in the international survey for the ACAMS Job Task Analysis, indicated that they performed the evaluation, implementation and operation of AML tools as a part of their job function.

CUSTOMER IDENTIFICATION AND DUE DILIGENCE

With respect to customer identification, the accessing or interfacing of various public records databases can serve to either authenticate identification presented (it must be recognized that original identification documents, including those issued by a government entity, may be obtained illegally and may be fraudulent – identity theft) or provide a means of non-documentary verification. Non-Documentary Verification is defined as methods used to verify identity other than relying on original documents. For example, where an individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the bank is not familiar with the documents presented; the account is opened without obtaining documents (some customers legitimately may be unable to present those customary

forms of identification when opening an account, for example, an elderly person may not have a valid driver's license or passport); the account is opened in a non face-to-face transaction (e.g. an account is opened by telephone, by mail, or over the Internet); and the type of account increases the risk that the bank will not be able to verify the true identity of the customer through documents (e.g. corporation, partnership, or trust). From a maintenance standpoint, management systems can also track and report the status of all documents, including those that are missing or expired.

Section 326 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, outlines three types of verification in this regard which can easily be facilitated by the use of technology. Such as, comparing the identifying information provided by the customer against fraud and bad check databases to determine whether any of the information is associated with known incidents of fraudulent behavior (negative verification); comparing the identifying information with information available from a trusted third party source, such as a credit report from a consumer reporting agency (positive verification); and analyzing whether there is logical consistency between the identifying information provided, such as the customer's name, street address, ZIP code, telephone number, date of birth, and valid social security number (logical verification).

Under Section 326 of the USA PATRIOT Act, the proposed rule also requires reasonable procedures for determining whether the customer appears on any list of known or suspected terrorists or terrorist organizations provided to the FSP by any federal government agency. Technology can be used to automate this comparison list checking with both governmental and other proprietary databases or watch lists.

In the area of customer due diligence, technology could be used to conduct Enhanced Due Diligence (EDD) by comparison list checking prospective high risk customers, such as politically exposed persons (e.g. senior foreign political officials), persons engaged in types of business activities or sectors known to be susceptible to money laundering (e.g. correspondent banking, Money Exchangers, Bureaux de Change, Internet Gambling, Money Remitters, electronic financial services, online casinos, cyber cash, and other non face-to-face financial services) and the financing of Terrorism (e.g. charitable, non-Profit, non governmental organizations of a religious, political, social or cultural nature). Additionally, lists can be checked for persons residing in, entities domiciled in, having substantial business in, and/or having funds sourced from countries identified by credible sources as having: inadequate anti-money laundering standards, jurisdictions that have been designated by the United States as a primary money laundering concern or have been designated as non-cooperative by an international body, or individuals and entities domiciled in high risk countries, representing a high risk for crime, drugs, terrorism and corruption, and and/or subject to international sanctions.

There are a variety of lists currently available by various governments and international bodies, such as the FATF Non-Cooperative Countries and Territories List, Financial Crimes Enforcement Network Advisories, Office of Foreign Assets Control, United Nations Sanctions, European Union Sanctions, Transparency International's Corruption Perception Index, the Central Intelligence Agency's Chiefs of State listing, and the U.S. Department of State's International Narcotics Control Strategy Report to name just a few. There are also several

proprietary and third party databases compiled from news media and other public sources that specifically identify individuals or entities worldwide that are known, suspected or substantially alleged to be involved in, either directly or indirectly, money laundering, fraud, drug trafficking, terrorism, public corruption, or subject to official sanction.

The future of the application of technology to this area of customer identification and due diligence may well be in relation to the proposed Section 326 regulation of the USA PATRIOT Act which allows for "similar safeguards" in the identification and verification process. Ultimately, this would enable FSPs to permit the use of any biometric identifiers that may be used in addition to, or instead of, photographs, for example.

MONITORING

Once the identification and verification procedures have been completed and the client relationship is established, FSPs should monitor the conduct of the account/relationship to ensure that it is consistent with the nature of business stated when the account/relationship was opened. To the end, FSPs are expected to have systems and controls in place to monitor on an ongoing basis the relevant activities in the course of the business relationship. The nature of this monitoring will depend on the nature of the business. The purpose of this monitoring is for FSPs to be vigilant for any significant, unexpected and unexplained change in the behavior of an account or inconsistencies in amount, origin, destination, or type with a customer's known legitimate activities. This inconsistency in the pattern of transactions is measured against the stated original purpose of the accounts.

Technology could be implemented to monitor possible areas such as: transaction type, frequency, amount, geographical origin/destination, and account signatories. It is often recognized that the most effective method of monitoring accounts is achieved through a combination of computerized and human manual solutions (a corporate compliance culture, and properly trained, vigilant staff through their day-to-day dealing with customers, will form an effective monitoring method as a matter of course). Computerized approaches may include the setting of "floor levels" for large cash transactions, high turnover or thresholds for monitoring by amount, by class or category of account, account profiling, wire transfer screening and by analyzing transaction patterns.

At the monitoring stage, it would be desirable for FSPs to incorporate any anti-fraud mechanisms or detection systems for check kiting, check counterfeiting, etc. in addition to dealing with anti-money laundering issues. The more robust and well rounded a monitoring system is, potentially the more valuable it can be to the institution. Furthermore, the ongoing nature of monitoring can allow for comparison list checking on a monthly basis against all account holders since last checked and not just at the time of the opening of the account.

Transaction monitoring has by far been the most popular and prevalent solution offered by technology vendors to date. Typically, this suspicious transaction detection software utilizes detection and discovery algorithms. Detection algorithms match the institution's information

with predictive models and profiles or pre-programmed idea of what a suspicious transaction could be. Discovery algorithms apply artificial intelligence techniques by finding new patterns that fall outside the usual pattern and/or refine the original predictive model. Lastly, this technology communicates the output and can assist with workflow and case management as human intelligence deals with the red flags generated by the system. The level of human intervention required also varies by product.

REPORTING

In the area of reporting, management exception reports can be printed and reviewed on a regular basis for certain high risk clients and/or transactions. Emerging best practice has sought the use of a highly secure network to allow financial institutions to electronically file Currency Transaction Reports (CTR's), Suspicious Activity Reports (SARs) via an Internet-based e-filing system, such as the Patriot Act Communication System, or PACS, as developed by the FinCEN in the U.S. In those cases, where the national reporting authority does not provide such a mechanism, FSPs can develop a private intra network between themselves and the reporting authority. This network could conceivably carry the responses to requests for production and regulatory requests.

TRAINING

The communication of a FSP's policies and procedures to prevent money laundering and the training on how to apply those procedures, underpin all other anti-money laundering strategies. A documented training program is essential and any training provided to staff should be certified. Most jurisdictions do not specify the exact nature of training to be given to staff, and therefore each FSP can tailor its training programs to suit its own needs, depending on size, resources and the type of business they undertake. Employees should be trained in a timely manner and prior to the opening of new accounts or the handling of any transactions. Over time, there is a danger that staff may become less vigilant concerning money laundering, and therefore it is vital that all staff receive appropriate refresher or recurrent training to maintain the prominence that money laundering prevention requires, their obligations arising from it and that they fully appreciate the importance that their employer places on it. As such, training should be held on a regular basis, at least annually, and in the case of operations personnel, perhaps more frequently. Depending on the number of employees an FSP has, this can be a daunting process.

FSPs could consider enterprise wide solutions such as computer or web based training to facilitate the process. Best practice has been to move away from CD-Rom based products which remove the issues of packaging and distribution and the risks and costs associated with loading software on desktops and/or over existing networks. In addition, a web based product allows for the course material to be current which is critical with ever changing regulations, legislation and guidance. Besides being designed to be highly interactive to increase comprehension and maintain employee interest, other features that can be built-in are bookmarking to remember where the user left off during multiple sessions, diagnostic tools to monitor the employee's course progress and remedial issues, content management to incorporate an FSP's own internal

policies and procedures, assessment which allows for testing, and a certification printing or tracking option to document completion for regulatory purposes.

RECORD KEEPING

Often the only valid role a financial institution can play in a money laundering investigation is through the provision of relevant records particularly where the money launderer has used a complex web of transactions specifically for the purpose of confusing the audit trail. FSPs should keep appropriate records relating to the evidence of client identification, the verification of identity, and records of transactions. Client identification consists of the identifying information, provided by the customer, the type of identification document(s) reviewed, if any, the identifying information and identification number of the document(s), and a copy of the identification document(s) itself. Verification records relate to the means and results of any additional measures undertaken to verify the identity of the customer and the resolution of any discrepancy in the identifying information obtained. Adequate records identifying relevant financial transactions should also be kept. Typically, these records must be maintained by the FSP for five years after the date the account is closed. Where there has been a report of a suspicious activity or the FSP is aware of a continuing investigation into money laundering relating to a client or a transaction, records relating to the transaction or the client should be retained until confirmation is received that the matter has been concluded. Best practice has found that document management and archiving systems (e.g. digital imaging) are effective in retrieving files for production requests in a timely and cost effective manner. There are a variety of software packages available to manage the images, whether the FSP does their own scanning or out sources the scanning to a scan house. Access to records could be web or network enabled and also be secured through the use of compartmentalized encryption, including access for only authorized persons by biometric devices.

Regardless of whether these additional applications of technology are implemented and in turn create additional records, normal vital business records are critical to the operation of the business and will need to be protected. Current technology is particularly effective in the area of disaster recovery such as with data replication and various fail over systems. As more and more regulators around the world require a business continuity program as a condition of the license holder, business continuity becomes less and less of an option.

CONCLUDING THOUGHTS

While some vendors offer hardware, others offer only a software based solution, and even other vendors that offer services on-line. The price tag for these solutions can range from the relatively inexpensive to the extremely expensive. Some systems can amount to several million dollars in the first year. Regardless of cost, all of these products have experienced a massive upsurge in business since the terrorist attacks of September 11, 2001.

No matter what the product, an FSP should not rush to judgment. The application of new technology is not always the solution to every problem; it does have limitations and should not be the first course of action. Besides the expense, it is incumbent on the FSP to determine

whether it is sufficient to leverage existing systems which may decrease the eventual reliance on new technology. For example, most compliance management reports can be generated from the output of existing systems. Failing the use of existing systems, clearly the most successful business model will incorporate a project management approach. There must be a clear specification of what is needed and how it will suit the needs of the FSP. Besides handling the myriad of implementation issues, the effectiveness of the application will largely depend on how well the new technology is integrated into existing systems.

There is no question that an FSP can achieve a greater degree of compliance as well as save time and money through the effective use of technology, this is especially true the larger the institution. Eliminating or reducing the compliance burden becomes even more imperative, not just from a regulatory compliance standpoint, but from a business standpoint as it becomes more and more difficult to drop profit to the bottom line as institutions face increasingly tighter margins.

Kenneth L. Bryant, MSCJ, CPP, CFE, CRP, CAMS, ACoI., and has more than fifteen years senior management experience as a money laundering and fraud investigator, compliance officer/money laundering reporting officer, enforcement regulator, and as an anti-money laundering, counter terrorism and counter narcotics consultant. Ken is a professional charter member of ACAMS and currently serves on the ACAMS Certification, Education and Technology Task Forces. www.amlcft.com