HIGH-RISK COUNTRIES IN AML MONITORING

ALICIA CORTEZ
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. Introduction</td>
<td>3</td>
</tr>
<tr>
<td>II. High-Risk Countries</td>
<td>3</td>
</tr>
<tr>
<td>Customers</td>
<td>4</td>
</tr>
<tr>
<td>Products</td>
<td>7</td>
</tr>
<tr>
<td>Monitoring</td>
<td>8</td>
</tr>
<tr>
<td>Audit Considerations</td>
<td>8</td>
</tr>
<tr>
<td>III. Conclusion</td>
<td>10</td>
</tr>
<tr>
<td>IV. References</td>
<td>10</td>
</tr>
</tbody>
</table>
I. Introduction

This report provides information on the monitoring process that financial institutions have to develop and implement for detecting and reporting suspicious activity with emphasis on high-risk countries. Policies and procedures focused towards combating money laundering provide the foundation for this fight. They have to address the particular vulnerabilities to which the financial institution is exposed. Policies and procedures have to be enforced to serve their purpose. An audit function, independent of the parties responsible for the monitoring, should be in place and conducted on a periodic basis.

II. High-Risk Countries

Some countries and jurisdictions pose a high risk to financial institutions. For example, countries subject to Office of Foreign Assets Control (OFAC) sanctions, countries identified as supporting international terrorism, jurisdictions determined to be of primary money laundering concern and subject to special measures, offshore financial centers (OFC), and jurisdictions or countries with deficiencies in combating money laundering and terrorist financing identified by international entities such as the Financial Action Task Force on Money Laundering (FATF).

Information about countries can be found in major newspapers, newsletters, account officers, hemispheric agencies and organizations, The World FactBook, Rundt’s World Business Intelligence, World-Check, and other publications. Transparency International provides the Corruption Perception Index (CPI).

OFAC maintains lists of countries, entities and individuals associated with terrorism, money laundering and other sanctioned activities. The OFAC countries list is compiled based on national security and United States foreign policy goals.

The Financial Action Task Force identifies jurisdictions that have strategic AML/CFT deficiencies and to which countermeasures apply, and jurisdictions with strategic AML/CFT deficiencies that have
not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies. Each jurisdiction presents different degrees of ML/FT risks. A list of high-risk countries can be found on the FATF website.

A financial institution should consider the characteristics of foreign countries such as growth, debt, currency, inflation rate, tax rate, banking system, stability and type of government, as well as corruption, terrorist and criminal activity. Some countries make it difficult for the people to move their money out of the country, or have strict currency exchange policies. Individuals and businesses will look for alternatives to safeguard their money.

Financial institutions must be aware of jurisdictions that have been rated high risk or non-cooperative, and take this information into consideration when selecting their target markets. Maybe the institution is willing to handle a certain level of risk, and include some high-risk jurisdictions in the target market selection.

Recent FATF publications indicated that Argentina, previously identified by FATF as having AML/CFT deficiencies, has been working to correct some deficiencies. However, other deficiencies have not been addressed, which relate to the criminalization of money laundering and suspicious transaction reporting requirements.

The FATF also published that Bolivia had improved its AML/CFT controls and corrected the previously identified deficiencies. As such, this country is no longer subject to FATF’s AML/CFT compliance monitoring process.

Although FATF identified Mongolia as having improved its AML/CFT controls, the country has not made sufficient progress and some deficiencies remain. Mongolia is encouraged to continue working to address the remaining deficiencies.

CUSTOMERS

Different types of individuals and businesses in any high-risk country may seek a relationship with a financial institution in the US. Each type of customer presents different characteristics and poses different levels of risk depending on the nature of business, occupation, or activities. They have different reasons and different needs for establishing a relationship. An example of high-risk customers follows.
Foreign banks and foreign money service providers may want to have access to the US financial system, whose products and services may not be available in their countries or are available but are more economically favorable in the US.

Non-bank financial institutions are different in size and volume of business and have a diversity of customers, and therefore, these institutions pose different levels of risks to a financial institution. The fact that these businesses may not maintain an ongoing relationship with the customer increases the risk due to the lack of identification requirements.

Senior foreign political figures and their immediate family members and close associates (politically exposed persons or PEPs) establish relationships at financial institutions in the US to move their money out of their countries.

Foreign corporations, offshore corporations, Private Investment Companies (PIC), and international business corporations (IBC) located in higher-risk geographic locations pose a higher risk because it is more difficult to ascertain the validity and adequacy of the documents presented, and to be familiar with the laws and requirements of foreign jurisdictions.

Foreign individuals use financial institution products and services for asset preservation, business expansion, and investments.

Characteristics of foreign individuals may involve:

- Need of confidentiality and privacy. The individual may be concerned about the security of the family. This may motivate an individual to open and maintain accounts at US financial institutions.
- Infrequent physical contact with the financial institution due to the increased use of the fax, email and online financial services. These methods of contact prompt the financial institution to require additional verification of signature on documents sent by fax and call backs to confirm customer instructions.
- High net worth individuals may be concerned with inflation or the devaluation of currency in their countries and want to move funds out of their countries. Investment opportunities are also a reason to maintain accounts at the US.

In order to predict the types of activity in which the customer is likely to engage in, a customer due diligence process is needed.
The process begins with verifying the customer’s identity and assessing the risks associated with that customer. The identification process also includes screening customers against OFAC sanction lists, PEP lists, and other lists of adverse information. Screening should also be performed in an ongoing basis so new and established customers are compared against new parties added to the lists.

Identifying information obtained at account opening also includes details on the customer’s line of business or occupation, financial resources and expected activity (type and volume of transactions). This information provides an understanding of the anticipated flow of funds in and out of the account and allows a risk rating of the customer, which in turn, facilitates the detection and reporting of suspicious activity.

A customer profile is created based on the information obtained. It is very important to keep the customer information current by periodically contacting the customer, reviewing activity reports, obtaining explanation of changes in activity, and incorporating the information into the existing profile. A risk rating is assigned to the customer based on the profile.

Enhanced due diligence is applied to customers that have been identified as presenting higher risks. For example, periodic visits by the account officer to the customer’s place of business are an excellent source of information about the business financial situation, assets, operations, their customers, stability, legitimacy of business, etc., as well as review of financial information and strict scrutiny of activity.

Officers’ knowledge and experience are another valuable source of information about the customers and their countries of operations. An experienced account officer can detect any unusual behavior and alert the appropriate department in the financial institution that is responsible for monitoring customers’ activity, detecting and reporting suspicious activity.
PRODUCTS

Products with different levels of risk are offered by financial institutions to their customers. Products that pose higher risks include:

- Electronic funds payment services (e.g., prepaid and payroll cards), funds transfers (domestic and international), automated clearing house (ACH) transactions, and automated teller machines (ATM). These products facilitate customers’ transactions, but also increase the risk to the financial institution. It is more difficult to identify the conductor, and the transactions are processed immediately. Funds transfers may involve high-risk countries and jurisdictions.

- Cash Management Services (online financial services, remote deposit capture, and lock-box deposits and payments) provide a means for the customers to remotely process their transactions without the need to visit the financial institution or contacting the account officer.

- Pouch activity offers foreign customers the convenience of sending their transaction requests and documentation to the financial institution via courier. This product allows individuals and businesses to remotely open and maintain accounts at US financial institutions, unless the US financial institution requires a face-to-face contact with the prospective customer before opening any type of account.

- The remote deposit capture (RDC) is an alternative to the pouch activity since the customer is able to process their check deposits at their own place and time. An increased risk to fraud is present if the item is altered or deposited multiple times.

- Demand Deposit Accounts are a traditional product offered by the financial institution that does not draw special attention; however, if it is misused it can provide a means for criminals to hide the proceeds of drug trafficking, political corruption, or any other illegal activities. This type of account provides terrorists with a convenient place to maintain the funds they need to finance their specific terrorist activities.

- Wealth Management services are provided to high net worth customers, usually foreigners, visiting the financial institution occasionally, probably in transit to vacation places or in a business trip. This category may include PEPs and beneficial owners of high-risk businesses.

- Monetary instruments may be used in the placement and layering stages of money laundering to conceal the proceeds of illicit activities.

- Foreign correspondent accounts may expose the US financial institution to increased risks to transactions involving payable through accounts or nesting activities because the foreign correspondent financial institution may have
relationships with other foreign financial institutions that permit those activities. The customers of the foreign correspondent institution do not have direct access to the domestic correspondent account. This is different than payable through accounts, in which the foreign institution provides its customers with checks from the domestic financial institution. These transactions provide anonymity to conductors, who have become authorized signers on the domestic account. To reduce the risk, the US financial institution may allow the opening of correspondent accounts with selected foreign financial institutions only. The Wolfsberg Group of International Financial Institutions issued several principles as guidance for corresponding banking relationships including the implementation of policies and procedures, approval of the correspondent relationship, independent review for compliance with policies and procedures, and risk-based due diligence.

- Lending activities, particularly loans secured by cash collateral and marketable securities. Time deposits are widely used to secure loans. A money launderer may open a time deposit with illegal money and obtain a loan with the purpose to hide the true source of the funds.

**MONITORING**

A system to monitor the customers’ activity is critical for detecting and reporting suspicious activity. Adequate policies and procedures are developed according to the institution’s risk profile, which considers its location, size, customer base, and volume of activity. Monitoring systems may be manual, automated, or a combination of those and should include country, customer, and activity. As such, it must incorporate the lists of high-risk countries. Automated monitoring systems should be validated by an independent party to verify they are working as intended and are producing useful alerts.

**AUDIT CONSIDERATIONS**

An independent audit must include a review of the policies and procedures covering the monitoring process, the method the institution uses for identifying high-risk countries in its monitoring systems, and the extent of analysis performed on the generated alerts. The auditor has to review and understand the process in order to be able to perform appropriate testing. A preliminary meeting with the designated parties responsible for the process is useful for clarifying any specific concerns they have pertaining to the function, which should be addressed during the audit.
A review of the results of prior audits and regulatory exams will help the auditor pay particular attention to the areas that have shown weaknesses in the past, and evaluate management’s efforts in correcting the weaknesses.

Verifying that the monitoring system has been validated by an independent party provides an adequate level of assurance regarding its performance; the methods for incorporating, maintaining and timely updating the lists of high-risk and sanctioned countries; proper approval and testing of system modifications; identification of transactions flowing through such countries; and the methodology for applying rules and producing alerts.

The auditor should also determine whether personnel in charge of the analysis of alerts (e.g. BSA analysts) are appropriately trained and adequately supervised; access to the automated system is granted according to their functions and properly approved; qualified personnel have been assigned the review of alerts; and an adequate escalation process is in place.

The testing stage of the audit begins by obtaining reports of alerts and cases that have been generated due to activity flowing through high-risk countries and jurisdictions of primary money laundering concern; verifying the accuracy and completeness of the population included in the reports; and selecting a representative sample of items from the source reports.

For the selected sample, the auditor should verify the review conducted by the BSA analyst to ensure it is comprehensive and properly documented, the decision to file or not a suspicious activity report is properly supported by the customer activity and the analysis, and the suspicious activity report (if warranted) has been filed on a timely basis. If the review performed by the BSA analyst does not appear adequate, the auditor must request additional explanations to clarify the situations or discrepancies noted and perform additional testing if deemed necessary.

When reviewing the customer activity, the auditor has to be attentive to red flags that suggest suspicious activities. For example, a business account that receives large deposits of cash or monetary instruments followed by cross-border wire transfers through high-risk jurisdictions; wire transfer activity without apparent business reason, when the source of funds cannot be verified, is inconsistent with the business, and involve high-risk jurisdictions; unusual transfers of funds among accounts of same holder through institutions located in high-risk countries; transfers routed through multiple foreign banks; international ACH transactions received from or sent to high-risk locations.
Documenting the work performed and properly organizing the work papers are integral parts of an audit. The identification of exceptions (violations, weaknesses and deficiencies) and the development of appropriate recommendations and corrective actions to address such exceptions are the responsibility of the auditor. A review of the test work and results must be performed by the audit supervisor. Exceptions noted and recommendations must be communicated to the responsible parties on a timely basis, as well as to the Audit Committee and the Board of Directors.

III. Conclusion

Adequate policies, procedures, and processes help the financial institution combat money laundering, terrorist financing, and other criminal activities. Identifying the customers, understanding their businesses and transactions, and establishing an effective monitoring system are essential in fighting money laundering and terrorist financing. The monitoring system should include an effective method to incorporate high-risk country lists and capture information on the activity flowing through them. An independent audit function identifies deficiencies that are communicated to the responsible parties for correction. If not corrected, such deficiencies expose the financial institution, its directors and employees to sanctions and penalties from regulatory agencies.

ACAMS – Training material for different live sessions and web seminars
http://www.fincen.gov
http://www.fatf-gafi.org/
http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx
http://www.ffiec.gov/bsa_aml_infobase/