2014

AML De-Risking: An effective method of plugging AML control failures?

Bukola Adisa

August 2014

Table of Contents

Executive Summary

Anti-money laundering (AML) control failures have gained a lot of press in recent times. There have certainly been widely documented instances of firms that have been subject to regulatory censures as a result of deficiencies identified within their AML control framework.

As the penalties and fines have increased, financial institutions have looked for ways to plug these control deficiencies. These have ranged from simple solutions such as hiring extra resources to more complex solutions such as radical changes to operational models and setting up extensive remediation programs.

The new trend called "de-risking" is one of such complex solutions embarked upon by some banks which aim to simplify the business models as well as reduce AML risks by exiting some products or client types or both.

Examples of sectors being exited by banks are embassies, money services businesses (MSBs) and foreign correspondent banks (FCBs). The rationalization behind this is that these client types/sectors pose a higher level of risk compared to the potential returns they generate. These client types are often denoted as higher risk client types who could expose the banks to potential regulatory censures and financial penalties.

However, in trying to reduce the exposure to the risks posed by these client types, banks embark on mass customer exit programs where existing relationships whole sectors and client types are terminated. For example, HSBC and Barclays Bank PLC have terminated banking relationships with the MSB sector. This approach creates problems for the entire financial system, which are outlined below:

- The terminated clients still require access to banking services and will move on to smaller unsuspecting banks or financial institutions that lack the resources and expertise needed to manage high risk customers.
- In large and complex banks, it is often quite difficult to ensure that the customers exited in one business line do not re-enter the bank via a different business line as system integration is often lacking.
- Mass exit of the same sectors amongst different banks could lead to the banks being accused of collusion which creates competition issues.
- Mass exit programs are very difficult and expensive to manage and it is very difficult to achieve consistency.

In essence, the effective application of know your customer (KYC) procedures and ongoing monitoring remain the most effective way of ensuring a strong AML controls environment.

AML De-Risking: What does it mean?

The practice of exiting customer relationships is not a new concept. Exiting customer relationships for whatever reason has always been a practice undertaken by financial institutions.

More recently however, the term “de-risking” has been more pervasive within financial institutions. This practice has become more prevalent as the regulatory landscape changes, in an era of increased regulatory scrutiny and heightened regulatory expectations.

According to the Cambridge dictionary, to “de-risk” means to make something safer by reducing the possibility that something bad will happen and that money will be lost.[1] This is a simplistic definition that when applied to the Financial Services Industry can be defined as the practice of exiting client relationships or certain business models on the premise that they present an unacceptable level of money laundering risk.

This practice has been intensified in recent times after the 2008-2009 financial crisis as a result of increased scrutiny on the crackdown on the flow of money tied to suspected terrorist activity, drug lords and tax evaders, which are believed to be passed through the banking system.

Enforcement actions have stacked up across the financial services industry, with AML settlements, including some sanctions violations, spiking to total $3.5 billion in 2012, from $26.6 million in 2011, according to the Association of Certified Anti-Money Laundering Specialists (ACAMS).

That jump includes a $1.9 billion fine on HSBC (HSBA.L) for its failures to stop hundreds of millions of dollars of drug money routed through it from Mexico.

Other examples of large monetary fines imposed on financial institutions for breaches of Money Laundering Regulations by U.S. domestic and foreign regulators include:

- **MoneyGram International Inc.** – In 2012, MoneyGram International Inc. was fined **$100 million** and entered into a deferred prosecution agreement (DPA) with the Justice Department for failing to maintain an effective AML program.

- **First Bank of Delaware** – In 2012, the FDIC and FinCEN levied financial penalties of **$15 million** against the bank, for violations of the Bank Secrecy Act (BSA) and AML laws and regulations. The Federal Deposit Insurance Corporation (FDIC) and the Financial Crimes Enforcement Network (FinCEN) determined that the bank failed to implement an effective BSA/AML compliance program with internal controls reasonably designed to detect and report evidence of money laundering and other suspicious activity.

[1] Cambridge dictionaries online

In addition, The Delaware Office of State Bank Commissioner terminated First Bank of Delaware's charter and the FDIC terminated its deposit insurance effectively putting the bank out of business.

- **TD Bank NA** – In 2013, the OCC announced a Consent Order for a **$37.5 million** Civil Money Penalty against TD Bank, N.A. FinCEN announced it had issued a concurrent **$37.5 million** CMP assessment, and the Securities and Exchange Commission issued a press release to announce a **$15 million** CMP and Cease & Desist order against the bank, and its filing of charges against former bank regional Vice President Frank A. Spinosa.

  The principal charges against the bank are that it failed to file a series of suspicious activity reports (SARs) relating to suspicious activity in connection with a $1.2 billion Ponzi scheme conducted by Scott Rothstein, who was sentenced to 50 years in prison for his involvement.[2]

- **JP Morgan Chase Bank NA** – In January 2014, news releases from FinCEN, the Office of the Comptroller of Currency (OCC), and the U.S. Attorney's Office for the Southern District of New York (SDNY) announced that JPMorgan Chase Bank, N.A. and various affiliates had admitted to BSA reporting violations and other BSA/AML compliance program deficiencies. FinCEN announced that it has fined JPMorgan Chase Bank, N.A., **$461 million** for willfully violating BSA by failing to report suspicious transactions arising out of Bernard L. Madoff's decades-long, multi-billion dollar fraudulent investment scheme.

- Large monetary penalties in enforcement actions are not restricted to U.S. regulators. In 2012, the Financial Service Authority (FSA) (now known as the FCA or Financial Conduct Authority) imposed a financial penalty of **£8.75 million** on **Coutts & Company (Coutts or the Firm)** for breach of Principle 3 (management and control) of the FSA’s Principles for Businesses which occurred between December 15, 2007 and November 15, 2010.

  The FSA stated that Coutts failed to take reasonable care to establish and maintain effective AML systems and controls in relation to customers that posed a higher money laundering risk than standard customers.

These large monetary penalties levied on financial institutions for failures in money laundering controls have resulted in the banks re-assessing and reviewing their risk appetites as well as their client base. The byproduct of this re- assessment is the now prevalent practice of ‘AML de-risking’ or mass customer exits.

[2] http://www.bankersonline.com/security/bsapenaltylist.html#tdbank

A large number of multinational banks now have dedicated firm wide customer exit programs in place where high-risk customers, client base or products are critically reviewed. Business profitability is weighed against increased money laundering risk and in several instances the decision is taken to exit some customer relationships. Examples of client relationships and products that have fallen prey to mass exit programs include: MSBs, foreign correspondent banks (FCBs) and foreign politically exposed persons (PEPs).

The Interaction Between the Risk-Based Approach and Management of High-Risk Clients

The USA PATRIOT Act requires financial institutions to take a risk-based approach when designing their Customer Identification Program (CIP). Similarly in 2013, the FCA, in defining the risk-based approach, said that:

> *Firms must put in place adequate and risk-sensitive AML policies and procedures. This means that firms have to identify and assess their money laundering risk and put in place systems and controls adequately to manage and mitigate this risk. Firms who apply a risk-based approach to AML will focus AML resources where they will have the biggest impact.*[3]

The risk-based approach means a focus on outputs. Firms are required to have policies and procedures in place in relation to customer due diligence (CDD) and monitoring, among others. The execution and interpretation of a risk-based approach will vary from firm to firm and this will be largely dependent on the nature of the money laundering risks they face and the type of products they provide to clients.

Applying a risk-based approach usually means that firms will need to be proactive in seeking out information regarding money laundering trends and threats from external sources such as law enforcement as well as relying on their own experiences and observations. This allows firms effectively to review and revise their use of AML tools to fit the specific risks that they face.

One of the key elements of a risk-based approach is the risk ranking of certain customers into different risk classes. Again, these classes vary amongst firms. Some firms designate different classes of risk by designating clients as high, medium and low.

Others may use a numbering or rating system from one to five where one is low risk and five is the highest risk category as seen in the figure on the opposite page:

[3] http://www.fca.org.uk/about/what/protecting/financial-crime/money-laundering/approach

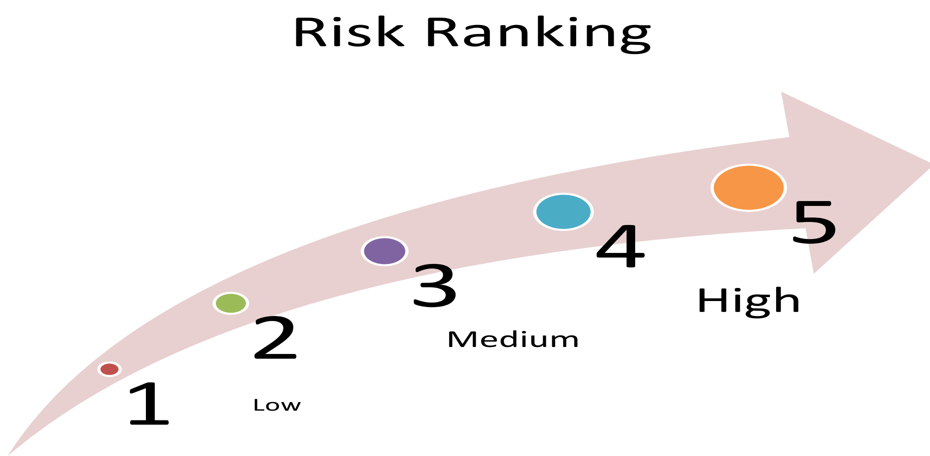

Figure 1: Risk Ranking of Clients

The reasons why clients are risk ranked as part of executing a risk based approach is to ensure that:

- The proper level and depth of due diligence is performed on the client
- The proper level and depth of ongoing due diligence is performed on the client
- The level of transaction monitoring performed on the client's transactions is of the appropriate rigor.

Several factors drive a financial institution's customer risk ranking/risk assessment process. Typical factors will include:

- **Jurisdiction**: The Financial Action Task Force (FATF) maintains lists of jurisdictions with weak money laundering controls. They also maintain lists of territories which have little to no national laws focused on combating money laundering offenses. These territories are known as non-cooperative territories and regions. A customer who is based in one of these jurisdictions may need to be subject to a greater level of scrutiny which may result in a higher risk ranking.

- **Political status:** Clients who are PEPs in jurisdictions where money laundering is rife, with weak money laundering regulations and where corruption is endemic may present a higher level of risk. The definition extends to immediate family members and known close associates. The due diligence and ongoing monitoring required with these types of clients may necessitate them being risk ranked with a higher risk category.

  In addition, individuals or entities that are adversely portrayed in the media, with a lot of negative media attention focused on them may be designated as higher risk due to the potential increase in reputation risk for the financial institution.

- **Industry type**: Risk ranking is also driven by the type of business the clients are engaged in. FATF recommendations have identified certain industries and professions that are susceptible to the risk of being used to facilitate money laundering. Examples of such industries are:

- Dealers in precious metals and stones
- Trust and company service providers
- Embassies
- MSBs
- Casinos
- Internet-based payment services businesses

Due to the nature of the business conducted in these industries, a financial institution may need to designate any potential client operating in these industries as high risk so that the appropriate level of due diligence and monitoring can be applied.

- **Product type**: Some products, by their nature present a higher level of risk to the bank. In this case, any client wishing to transact in these products and any transactions involving these products may be subject to enhanced scrutiny so as to detect any potential suspicious activity. Examples of such products include:

- Foreign correspondent banking
- Remote deposit capture
- Prepaid cards
- Electronic funds transfer
- Private banking

In essence, the regulations do not prohibit a financial institution from entering into a customer relationship with any of the client types that present a higher level of risk. Conversely, the regulations also do not prohibit a financial institution from providing products or services that are susceptible to the risk of money laundering. The requirement for financial institutions is to ensure that in taking on clients, offering products and conducting their business that they do this with a risk-based approach.

This risk-based approach, as defined by the financial institution may give rise to certain obligations such as risk ranking, screening, etc. For example Section 312 of the USA PATRIOT Act requires banks with private banking clients to conduct enhanced due diligence (EDD) if their client is a PEP. To do this, the onus is on the financial institutions to correctly identify and designate PEP relationships.

Historically, some financial institutions have defined their risk appetites in onboarding clients and have offered products and services to clients across all risk spectrums. In certain instances, the firms, having entered into client relationships with customers on the higher end of the risk spectrum have then failed to design and implement adequate controls to monitor those clients on an ongoing basis.

Over time, however, regulators have noted the control deficiencies in managing high-risk customers and have applied penalties and enforcement actions, some of which were summarized above. It is worthy to mention that in June 2011, the U.K. financial regulator (FSA as it was known then) published a paper which outlined the results of a thematic review it had conducted on a sample of banks under its supervision. The paper was titled *Banks' Management of High Money-Laundering Risk Situations*. [4]

The FSA report focused in particular on correspondent banking relationships, wire transfer payments and high-risk customers including PEPs. Three summarized findings in particular within this report are relevant:

1. Some banks appeared unwilling to turn away or exit very profitable business relationships when there appeared to be an unacceptable risk of handling the proceeds of crime. Around a third of banks, including the private banking arms of some major banking groups, appeared willing to accept very high levels of money laundering risk if the immediate reputational and regulatory risk was acceptable.

2. Over half the banks we [FSA] visited failed to apply meaningful EDD measures in higher risk situations and therefore failed to identify or record adverse information about the customer or the customer's beneficial owner. Around a third of them dismissed serious allegations about their customers without adequate review.

3. Some banks' AML risk-assessment frameworks were not robust. For example, we [FSA] found evidence of risk matrices allocating inappropriate low-risk scores to high-risk jurisdictions where the bank maintained significant business relationships. This could have led to them not having to apply EDD and monitoring measures.

From the above findings of the review conducted by the FSA on the management of high-risk customers, it is easy to see how an ineffective risk assessment or risk scoring model leads to the failure to apply the appropriate level of due diligence required.

The risk assessment process, inclusive of an effective risk scoring model is integral to the money laundering prevention framework. This is because if the right risk scores are applied, the customer will be correctly designated into the right risk category. Following this, the appropriate level of due diligence will be applied. This will hitherto lead to the correct level of ongoing customer monitoring including transaction monitoring being applied.

[4] http://www.fca.org.uk/your-fca/documents/fsa-aml-final-report

Effective AML Controls

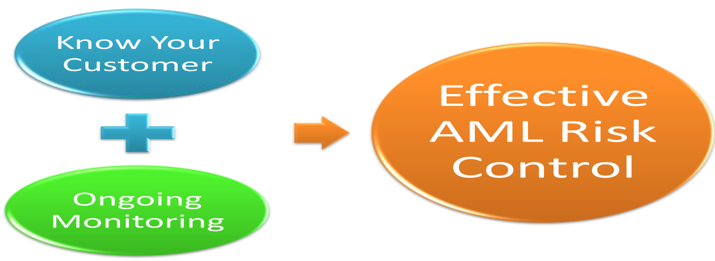

Figure 2: Effective Controls

Know Your Customer: The Gatekeeper and Preventative Control

The premise of this paper is not to say that mass de-risking programs are ineffective and are the wrong course of action to adopt in certain circumstances.

However, what this paper sets to highlight and explore is the fact that had proper controls been implemented at the outset, then the need for mass customer exits would be limited. As noted earlier, exiting customer relationships is a course of action that has always been available to financial institutions. Banks and other financial institutions exit customer relationships, not only for financial crime risks reasons but in certain cases, for genuine business reasons.

However, key regulators all over the world such as the OCC and the FCA have always made it clear that “effective KYC controls still remain the most effective deterrent of money laundering and financial crime.”

According to the Basel Committee on Banking Supervision (BCBS), supervisors around the world are increasingly recognizing the importance of ensuring that their banks have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate due diligence on new and existing customers is a key part of these controls. Without this due diligence, banks can become subject to reputational, operational, legal and concentration risks, which can result in significant financial cost.

The existence and correct application of robust KYC standards and accompanying procedures is an effective way of ensuring that only the right type of customers are on-boarded. The view held is that if only the right customers are allowed in the first instance, there would be no significant money laundering issues or risks throughout the life cycle of the relationship.

When money laundering risk crystallizes, often as a result of control gaps and failures, and enforcement actions are applied by the regulators and government agencies, the firms involved are then in a position where they have to review their controls and apply remedial actions.

A particular area where this is prevalent is in KYC remediation. This occurs when a regulator or internal audit has identified control gaps or failures in KYC controls and has recommended that the controls be plugged or fixed. This can be for a number of reasons, for example,

- Failure to obtain accurate KYC documents at onboarding
- Failure to refresh the documents obtained at onboarding
- Lack of evidence of extra due diligence conducted in higher risk situations/ customers.

In practice during remediation, banks have the opportunity to review their client base and in these instances, they weigh the business benefits of keeping a client on the books against the risk they present and where the regulatory risks are deemed unacceptably high, the decision is taken to exit the client relationship.

However, if the proper KYC onboarding procedures had been applied at the earlier stages, there may be no requirement for a KYC remediation program and ultimately a mass customer exit program.

It is in this regard that a robust KYC program is deemed to be a very important preventative control as it acts as an effective filter and prevents costly remediation programs as well as enforcement actions further down the line.

Sound KYC policies and procedures not only contribute to a bank's overall safety and soundness, they also protect the integrity of the banking system by reducing the likelihood of banks becoming vehicles for money laundering, terrorist financing and other unlawful activities.

Ongoing Monitoring: The Detective Control

As effective as rigorous KYC and CDD checks may be, it is possible that banks may inadvertently onboard customers who may turn out to have unacceptable high-risk profiles. This may happen for a number of reasons including:

- Customer providing false information or forged documentation
- Incorrect risk scoring applied leading to a lower level of due diligence checks
- Bank hitherto had a different level of risk tolerance which changed after onboarding

It is due to the possibility of the above scenarios occurring that banks have to ensure that ongoing refresh of customer information as well as monitoring of customer transactions are in place. The rationale is that this will catch any risk factors that were missed at customer onboarding.

Ongoing monitoring is an essential aspect of effective KYC procedures. Banks can only effectively control and reduce their risk if they have an understanding of normal and reasonable account activity of their customers so that they have a means of identifying transactions which fall outside the regular pattern of an account’s activity.

Without such knowledge, they are likely to fail in their duty to report suspicious transactions to the appropriate authorities in cases where they are required to do so.

For all accounts, some level of monitoring should be put in place, which should help in detecting and reporting suspicious activities to the relevant authorities. However, for higher risk accounts, intensified and more robust monitoring methods should be applied. According to the BCBS, for higher risk accounts:

- Banks should ensure that they have adequate management information systems to provide managers and compliance officers with timely information needed to identify, analyze and effectively monitor higher risk customer accounts. The types of reports that may be needed include reports of missing account opening documentation, transactions made through a customer account that are unusual, and aggregations of a customer's total relationship with the bank.

- Senior management in charge of private banking business should know the personal circumstances of the bank's high-risk customers and be alert to sources of third-party information. Significant transactions by these customers should be approved by a senior manager.

- Banks should develop a clear policy and internal guidelines, procedures and controls and remain especially vigilant regarding business relationships with PEPs and high profile individuals or with persons and companies that are clearly related to or associated with them. As all PEPs may not be identified initially and since existing customers may subsequently acquire PEP status, regular reviews of at least the more important customers should be undertaken.[5]

When appropriate transaction monitoring procedures are applied, any detected suspicious activities arising from the monitoring activity should be reported to the relevant authorities. In addition to the reporting, banks will also conduct a review on the customer account while monitoring for and reporting further identified suspicious activities.

Dependent on instruction from the law enforcement agencies, a decision may be taken to either continue to monitor the activities of the customer or to exit the relationship. In coming to this decision, the risk scoring of the customer is reviewed along with relevant KYC documents.

Again, this goes to show that the appropriate mix of initial KYC preventative controls and ongoing monitoring detective controls will provide a framework for the management of high-risk customers. High-risk situations and customer types are mitigated by the application of EDD and enhanced monitoring. The decision to exit these relationships should be as a result of the outputs of both the EDD and enhanced monitoring.

[5] Basel Committee on Banking Supervision: Customer Due Diligence For Banks- October 2001

Case Study: Dahabshiil v Barclays Bank PLC

In May 2013, Barclays made the decision to terminate its relationship with money remittance companies. Dahabshiil was one of the organizations affected by the decision to exit that sector. According to Barclays, the decision was made under its risk-based approach to its obligations in compliance with AML regulations.

This decision had far reaching implications for Dahabshiil due to its extensive operations in Somalia. Following years of civil war, Somalia has been left without a functioning banking industry, and remittances sent to the country via transfer shops and kiosks are worth about $1 billion to $2 billion a year.

Dahabshiil had held bank accounts with Barclays over a period of 15 years during which Barclays had confirmed that the remittance company had satisfactory AML policies and procedures in place.

They did not single out Dahabshiil; they decided that dealing with money transfer companies—which are designated as higher risk from a money laundering perspective—was outside their risk appetite. With de-risking high on the regulatory agenda, a number of institutions have been reassessing their risk appetite and controls frameworks, and taking decisions to exit relationships that are perceived to pose a higher risk such as accounts held for PEPs, embassies and MSBs as well as foreign correspondent banking relationships.[6]

However, Dahabshiil Transfer Services obtained an interim injunction at the High Court against Barclays Bank, preventing Barclays from terminating its relationship with Dahabshiil on competition law grounds. The judge, in trying the case admitted that Barclays, like any other business is contractually within their right to exit customer relationships.

Dahabshiil has since commented that "as part of the agreement, there will be a transition period to allow Dahabshiil to end its banking relationship with Barclays and move to alternative arrangements. In the interim, we are putting in place alternative arrangements which will avoid any disruption in service to our clients."[7]

Barclays is not the only banking institution to exit the MSBs based on money laundering grounds. HSBC, in 2012 entered into a settlement for $1.9 billion over money laundering failings. Following that settlement, HSBC instituted an extensive de-risking program where all accounts held by MSBs were terminated with 30 days' notice.

---

[6] http://www.int-comp.com/blog/posts/2014/05/07/barclays,-dahabshiil-and-de-risking/

[7] http://www.dahabshiil.com/2013/11/dahabshiil-wins-injunction-against-barclays.html

Dahabshiil's injunction is an interim injunction, which only allows it time to find alternative arrangements. The question remains as to the effectiveness of willfully terminating these customer relationships. If it turns out that Dahabshiil or any of the other terminated MSBs were indeed conduits for money laundering and terrorist financing, then the entire system is still at risk as the risk has not been eliminated, merely transferred.

The monitoring and reporting of suspicious activities to regulators is of far more importance and value as the information provided from the detection of these activities could aid law enforcement agencies in the investigation and prosecution of money laundering offenses.

In exiting the entire portfolio of a certain client type, the ability to pass on this information is severely restricted especially if the MSBs or any other terminated high-risk clients become a client with another bank or financial institution. This risk is especially heightened if the new bank does not have adequate and robust money laundering systems and controls.

A holistic view of the money laundering risks present within the global financial system seems to be lacking when banks such as HSBC and Barclays embark on such programs as described above. If the view is indeed an all-encompassing and global view, then the decision to exit a client will be taken only after preventative and detective controls have been consistently applied. The holistic view will dictate that mass exits will not benefit the entire financial system as the risk will not go away.

Another interesting question to note is: What makes one sector a higher risk than another? And how is the decision made as to which type of customers get terminated and which types are kept? For instance, a number of global banks have been fined for breaches of money laundering regulations themselves. Are these relationships being terminated? Also are all PEP relationships being exited seeing that they are also high-risk client types? This underscores the subjective nature of de-risking programs and how it does not mitigate risks in a consistent manner.

Pitfalls of Mass De-Risking Programs

Mass de-risking and customer exit programs are fraught with risks and potential pitfalls. As stated above, terminating a client who carries on in business only achieves the outcome of the transference of the perceived risk as the client will tend to look for alternative ways of continuing in business.

De-risking programs have not escaped the attention of international regulators. At a recent ACAMS conference, a senior official from OCC decried the practice.

“De-risking can have serious consequences,” Dan Stipano, a senior OCC enforcement official, said at the event. He indicated that when large banks get out of the higher risk areas those customers can migrate to institutions that lack the resources and lack the expertise to manage the risk, a situation he described as an invitation to trouble.

“A lot of these higher risk businesses are attracted to community banks that are pressed for sources of revenue … in the current climate,” he said.[8]

What does de-risking mean for smaller unsuspecting players?

As highlighted above by the OCC, de-risking efforts by bigger banks could have potential negative implications for the smaller players or the community banks that are increasingly pressed for revenues in today’s highly competitive markets.

These banks may not have the level of staff resources and systems to effectively manage the risks posed by onboarding these higher risk businesses that have been exited by the bigger banks. In which case, the risks of the financial system being used to facilitate money laundering or terrorist financing offenses still remain within the entire system.

Corporate Memory: The Challenge of Ensuring a Complete Exit

Another challenge faced by the larger complex banks in de-risking their portfolio is in ensuring that a client is completely off-boarded. It can be operationally and logistically difficult to ensure that a client who has been exited within one line of business is terminated across all the other lines of business.

Also, it can be challenging to monitor and ensure that the entity either in its present form or in another form is not subsequently on-boarded in another area. Controls need to be put in place to ensure that the terminated entity, its beneficial owners and other associated entities are “remembered” in the system to prevent them from coming back as customers of the bank.

---

[8] http://www.moneylaunderingconference.com/2014/assets/docs/3-27-17-complinet.com.pdf

This challenge is very common within the big complex banks where there is no alignment to the systems and no holistic view of the customer. Where this is not appropriately managed, the terminated client or customer may return as a customer of the bank in another form, thereby rendering the de-risking exercise futile.

After De-Risking: Tightening the Controls Process

Another area where the mass exit programs can go wrong is where there is an inordinate amount of attention and focus given to terminating customer relationships without this leading to an enhancement in the overall controls environment.

For a de-risking program to be completely successful, the framework should include a separate work stream or program focusing on enhancing the risk assessment, KYC and monitoring controls. This would ensure that the controls are operating effectively and would make the de-risking process a finite one off exercise.

An enhanced controls environment, the operation of which is sustainable, would ensure that the control gaps which necessitated the de-risking program, are plugged. In addition, the expectation of the regulators is not for de-risking exercises to take the place of due diligence, customer evaluation and monitoring controls.

Competition Issues

The Dahabshiil case against Barclays was on competition grounds. Dahabshiil, as a remittance business was informed of the notice to terminate their business by Barclays. The reason provided by Barclays was a change in its eligibility criteria across the sector. However, at the High Court it transpired that the reason was as a result of a review carried out on the MSB sector triggered by HSBC exiting this sector in 2012.

The wholesale exit of some client types has been widely reported in the press. For example, certain banks are terminating MSBs, foreign PEPs, embassy accounts and foreign correspondent bank accounts. This could easily be interpreted as a business strategy move rather than legitimate AML risk concerns. This has been flagged by the U.K. regulator (FCA) who is mindful that some firms may use this as an opportunity to gain market foothold. According to Sharon Campbell from the FCA, the FCA will say something if firms are taking de-risking strategies because of competition issues.[9]

[9] http://compliancealert.org/five-firms-facing-possible-aml-enforcement-says-fca-official/

The Role of Internal Audit in Maintaining Effective AML Controls

A strong and independent internal audit department is central to the development of a robust controls environment.

The role of the audit department in identifying control gaps and working with the business to remediate these gaps has been strengthened by the regulators. For instance, audit departments have been subject to criticisms by the regulator in recent times for failing to identify and flag AML control deficiencies within the business.

Internal audit is in a unique position in terms of being an entirely independent function, free from business control, which increases the value placed on the audit opinion.

De-risking could be beneficial to a firm's control framework if run properly. Having to exit clients on a wholesale basis is not an ideal situation to be in for financial institutions. However, firms recognize that KYC controls have not been adequate and the risk appetite, which was historically deemed sufficient, is not enough in today's environment of heightened regulatory expectations.

In that regard, some firms are left with no choice but to reduce their risk profile by exiting relationships that are no longer tenable. Internal audit has a vital role in ensuring that the right balance is achieved between exiting high-risk client relationships and ensuring that the controls environment remains robust, some of which are outlined below:

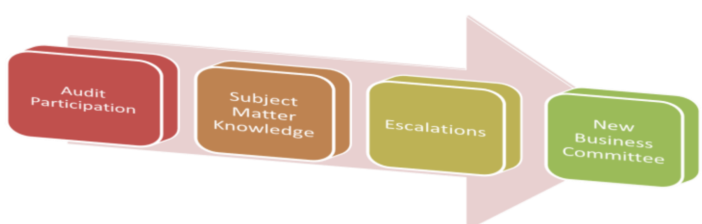

Figure 3- Role of Internal Audit

- **Audit participation at committees**: In a lot of instances, internal audit attends the committee meetings where the de-risking activities are discussed for particular lines of business. This presents an opportunity for audit to contribute to the discussions to ensure that the right decisions are taken at those meetings. Audit opinion carries a lot of weight and should be used appropriately.

- **Subject-matter knowledge**: When audit is able to speak knowledgeably about AML regulatory matters and issues, the value they add to the business line is increased. In the area of de-risking especially, specialist knowledge of onboarding, risk assessments and customer exits are very beneficial.

- **Escalations**: In regular stakeholder engagements, audit has the opportunity to ensure that any concerns they have about any aspect of the AML control framework is raised to the relevant people. If there are concerns that the de-risking activities are not tying back to a strengthening in the KYC control framework, audit should be raising this and ensuring that the enhancement of controls remain an agenda.

- **New business committee**: Where audit is invited to participate at the new business approvals committee, there is an opportunity to contribute to these assessments from a controls perspective. This will ensure that a product fraught with risk is not approved which will require remedial action further down the line.

In summary, from the above it is apparent that the contributions and opinions of an independent internal audit function can go a long way in improving and enhancing the overall controls framework within a firm.

Final Thoughts

The Preferred Model for Mitigating AML Control Failures

> *You shouldn't feel that you can't bank a customer just because they fall into a category that on its face appears to carry an elevated level of risk. Higher risk categories of customers call for stronger risk management and controls, not a strategy of total avoidance.*
>
> *Obviously, if the risk posed by a business or an individual is too great to be managed successfully, then you have to turn that customer away. But you should only make those decisions after appropriate due diligence*[10]

- **OCC Comptroller Curry ACAMS Conference, Hollywood March 2014.**

The FCA "would rarely expect" firms to exit business relationships to avoid risks. (She said that this was unlikely to be the only solution to the problem). "We don't want to end up in a world where the fear of the consequences … will deny people access to legitimate services.[11]

- **Tracey McDermott, FCA director of enforcement and financial crime. SWIFT Business Forum**

The two quotes above are from two of the biggest regulators of financial institutions (The OCC in the U.S. and the FCA in the U.K.). Of particular interest is Comptroller Curry's statement that higher risk clients should be subject to enhanced controls and not an avoidance strategy.

As stated earlier, there are provisions in the law and regulations for applying EDD and more stringent monitoring to higher risk clients. The model of applying strong KYC preventive controls and target monitoring detective controls should be applied in the management of high-risk customers.

The three lines of defense of the business, the control functions and internal audit all have a role to play in ensuring that firms are not used to facilitate money laundering and terrorist financing offenses. It all begins with the company defining its risk appetite and correctly risk assessing and scoring customers. This should then be followed up by the appropriate level of due diligence being applied to the customer. All these approaches married with the appropriate monitoring and reporting controls leads to an

---

[10] http://www.moneylaunderingconference.com/2014/assets/docs/3-27-17-complinet.com.pdf

[11] http://www.complinet.com/global/news/news/article.html?ref=171592

effective and robust controls environment which does not require complex, expensive and lengthy remediation efforts.

As Dan Stipano, a senior OCC enforcement official put it at the ACAMS conference in Hollywood, “But we also don't think … that the answer, when it comes to providing banking services for higher risk clients, is to just dump them wholesale."

On a positive note, de-risking initiatives could be beneficial to a firm’s operating model. In streamlining and simplifying business models, a firm becomes more agile and more efficient. Operational efficiencies are also achieved when a business focuses on a smaller number of products and/or customer types.

From a BSA/AML perspective, de-risking aids the strategic thinking and planning for AML risks. This is because a firm that is engaged in a de-risking exercise is more likely to view AML risks differently. When the output from this exercise is linked with the Risk Assessment process, the AML controls environment is improved and strengthened.

Resources

1. http://www.bankersonline.com/security/bsapenaltylist.html#tdbank
2. FCA Financial Crime Guide, Parts 1&2
3. The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation
4. FSA Banks' Management of high money-laundering risks situations
5. Basel Committee on Banking Supervision: Customer Due Diligence For Banks- October 2001
6. www.complinet.com
7. http://www.fca.org.uk/about/what/protecting/financial-crime/money-laundering/approach
8. http://www.fca.org.uk/your-fca/documents/fsa-aml-final-report
9. http://www.dahabshiil.com/2013/11/dahabshiil-wins-injunction-against-barclays.html
10. http://www.moneylaunderingconference.com/2014/assets/docs/3-27-17-complinet.com.pdf
11. http://www.moneylaunderingconference.com/2014/assets/docs/3-27-17-complinet.com.pdf
12. www.ft.com
13. http://www.int-comp.com/blog/posts/2014/05/07/barclays,-dahabshiil-and-de-risking/