THE CONCEALED INTERNAL THREAT: THE NEED TO MANAGE AFFILIATES AND AFFILIATE NETWORKS FOR ANTI-MONEY LAUNDERING RISKS

Dr. William Scott Grob, CAMS

March 2019

ACAMS®

Table of Contents

The Concealed Internal Threat

The role of correspondent banking continues to challenge regulators, correspondent and respondent banks, and the greater community of financial institutions connected to cross-border activity. Correspondent banking as defined by the Wolfsberg Group is the supplying of *financial accounts or banking services to another financial institution used to execute payments, trade finance, cash clearing, liquidity management, or lending to another bank's customer in a particular currency.*[1] While the Financial Action Task Force (FATF) and Wolfsberg Group continue to offer improved guidance and outreach, correspondent banking risks remain elevated.[2,3]

The critical challenge for a large financial institution with branches and subsidiaries located worldwide is to have an anti-money laundering (AML) compliance program, sanctions program, and transactional activities that are sufficiently robust and consistent across all customers, products, and services. Variance in controls across an organization creates anti-money laundering and counter-terrorism financing (AML/CTF) control gaps that are easily exploited by criminals and terrorist organizations. Furthermore, due to varying levels of technology and internal expertise, investments in affiliates that AML controls across the networks tend to be under-appreciated. This white paper examines the management of affiliates as a source of correspondent banking risk that is often disregarded due to the concentration on managing external banking relationships.

Affiliate management is an often overlooked aspect of correspondent banking.[4] Although there has been a fair amount of guidance offered on correspondent banking over the years, little advice focused on managing the correspondent banking relationships on affiliates has appeared from FATF, Wolfsberg, and nongovernmental organizations, such as the World Bank, the

---

[1] Wolfsberg Group. (2014). Wolfsberg anti-money laundering principles for correspondent banking. Retrieved: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/8.%20Wolfsberg-Correspondent-Banking-Principles-2014.pdf
[2] Financial Action Task Force. (2012, February). FATF recommendations. Retrieved from: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html
[3] Wolfsberg op. cit.
[4] Ibid., page 1

International Monetary Fund, and the Asian Development Bank to improve leadership and financial inclusion. Financial crime risk (FCR) remains elevated in this area.

In 2017, Habib Bank relinquished its New York State banking license, as senior management in Pakistan was unwilling to make significant investments in infrastructure and personnel to curb financial crime risks in U.S. dollar clearing, fund transfers, check clearing, trade finance, and lending, which were utilized by customers of Habib's affiliate network executed through its U.S. branch.[5] In contrast to the Agricultural Bank of China, affiliates contributed to the lack of underlying payment transparency on ordering and beneficiary details on MT103 and MT202 SWIFT[6] messages facilitating USD payments or trade transactions.[7] The Financial Conduct Authority fined Deutsche Bank for masking high-risk customer trades between its Moscow branch and the UK center with mirror trades.[8] Correspondent banking relies on the electronic network. This paper recommends paying greater attention to the management of affiliates due to internal control weaknesses. A need exists to create standards and best practices around the internal transactional activity.

Problem Statement

A review of the enforcement actions issued by the New York State Department of Financial Services over 2018 referenced affiliate or branch problems within the consent orders of Société Générale, Standard Chartered Bank, Mashreqbank, and Nonghyup Bank.[9] The problem is more acutely applicable to foreign financial institutions with a USD clearing branch. However, the Financial Conduct Authority has fined banks, such as Deutsche Bank, Sonali (UK) Bank, Bank of Lebanon, and their respective money laundering reporting officers on GBP clearing, too. The Monetary Authority of Singapore fined Standard Chartered Bank for breaches

---

[5] New York State Department of Financial Services. (2017, August 24). New York State Department of Financial Services. Retrieved from Department of Financial Services Issues Against Habib Bank Limited and Habib Bank Limited, New York Branch: https://www.dfs.ny.gov/docs/about/ea/ea170824a.pdf
[6] Society for Worldwide Interbank Financial Telecommunication
[7] New York State Department of Financial Services. (2016, November 4). New York State Department of Financial Services. Retrieved from Department of Financial Services Issues Consent Order to Agricultural Bank of China Limited: https://www.dfs.ny.gov/docs/about/ea/ea161104.pdf
[8] Financial Conduct Authority. (2017, January 31). Financial Conduct Authority. Retrieved from FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings: https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure
[9] New York State Department of Financial Services. (2018, November). New York State Department of Financial Services. Retrieved from Enforcement Actions: https://www.dfs.ny.gov/industry_guidance/enforcement_actions_lfs

in AML due to the transfer of trust accounts from Standard Chartered Trust (Guernsey) to Standard Chartered Trust (Singapore) Limited.[10]

Danske Bank Estonia branch is a current issue. From 2011 to 2018, Danske Bank cleared billions of euros from its headquarters on behalf of the Estonia branch without much recognition of the AML/CFT risks, in part because the company built its controls to be outward-facing rather than inspecting its nonresident portfolio and internal transactions.[11] Moreover, in the Danske Bank example, the Estonia branch generated sizable suspicious activity reports, because of the collection of nonresident customers, mainly domiciled in the Russian Federation and the broader Commonwealth of Independent States, initially acquired from Sampo Bank in 2007.[12] Even with customers identified from the Russian and Azerbaijani Laundromat scandals, neither the Estonia branch nor headquarters took steps toward corrective actions.[13]

Despite numerous red flags and suspicious customer behavior, including the termination of a correspondent banking relationship from a U.S. financial institution, Danske's board of directors, executive board, chief executive officer, the chief financial officer, the compliance officer, and business heads ignored suspicious activity alerts, suppressed concerns originating from these accounts, and breached their legal obligation.[14] An internal whistle-blower within Danske Bank brought the matter to the attention of senior management and the Danish Financial Supervisory Authority.[15]

---

[10] Monetary Authority of Singapore. (2018, March 19). Monetary Authority of Singapore. Retrieved from MAS Imposes Penalties on Standard Chartered Bank and Standard Chartered Trust for AML/CFT Breaches: http://www.mas.gov.sg/News-and-Publications/Enforcement-Actions/2018/MAS-Imposes-Penalties-on-Standard-Chartered-Bank-and-Standard-Chartered-Trust-for-AMLCFT-Breaches.aspx

[11] Bruun & Hjejle. (2018, September 18). Investigations into Danske Bank's Estonian branch. Retrieved from Danske Bank: https://danskebank.com/-/media/danske-bank-com/file-cloud/2018/9/report-on-the-non-resident-portfolio-at-danske-banks-estonian-branch-.-la=en.pdf - Pages 5-10

[12] Ibid., page 3

[13] Ibid., page 33

[14] Danske Bank. (2018, May 3). Danske Bank. Retrieved from Danske Bank's management and governance in relation to the AML case at: https://danskebank.com/-/media/danske-bank-com/pdf/investor-relations/fsa-statements/fsa-decision-re-danske-bank-3-may-2018-.-la=en.pdf - Pages 7-16

[15] Ibid., page 4

Consequently, affiliate management is often an ignored problem within the correspondent banking AML/CTF framework. Despite being defined by Wolfsberg Group and other institutions; few best practices are shared. This paper attempts to set out some best practices.

This research examines the management of affiliates as a source of correspondent banking risk often overlooked within an AML/CTF framework, but necessary for a robust detection and deterrence program. The leaders of many financial institutions build their FCR controls to be outward-enabled. The analysis identifies various control weaknesses and inherent risks not typically incorporated into an institution's risk assessment. The paper investigates the best practices needed to manage affiliates to arrest the rising correspondent banking risks. The challenge leaves many financial institutions vulnerable to regulatory enforcement actions and possible fines, and financial crime risk frameworks vulnerable to professional money laundering organizations.

The Importance of Correspondent Bank Networks

Correspondent banking is necessary to connect the myriad financial institutions, and, given the dependence on the U.S. dollar, to facilitate payments and trade between customers in various countries. This financial network underpins the global economy. Correspondent banking relies on an extensive network of banks, including branches and subsidiaries of financial institutions. The international banking community united under the Wolfsberg Group requires financial institutions to converge on a set of correspondent banking standards and practices to reduce FCR in the ecosystem. Both FATF Recommendation 13 and Section 312 of the USA Patriot Act[16] require financial institutions to perform varying levels of due diligence upon the respondent banks and affiliates alike.[17,18] Ultimately, financial institutions need to harmonize their operating models around shared services and utilities while improving transparency and technology.

[16] USA PATRIOT Act is short for the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001."
[17] Wolfsberg Group, Op. cit.
[18] Financial Crimes Enforcement Network. (2015, December). Fact sheet|: Section 312 of the USA PATRIOT Act Final Regulation and Notice of Proposed Rulemaking. Retrieved from FinCEN: https://www.fincen.gov/fact-sheet-section-312-usa-patriot-act-final-regulation-and-notice-proposed-rulemaking

Purpose of Affiliate Entity Management

FATF Recommendation 13 highlighted the correspondent banks' responsibilities around providing services to respondent banks. When providing correspondent banking services, a financial institution is required to conduct due diligence to assess another bank's FCR controls and vulnerabilities; however, many financial institutions are not aware that this responsibility extends to the management of their affiliates.

The purpose of the research is to highlight the best practices emerging around affiliate correspondent banking practices from the second line of defense perspectives. Even before 2012, regulators designated affiliates, subsidiaries, and branches as needing oversight.[19,20]

Over the years, from HSBC to the recent problems with Danske Bank, a financial institution's branches and subsidiaries may expose the central clearing entity to a significant amount of cross-border risk. In HSBC's Statement of Facts around its U.S. Department of Justice Deferred Prosecution Agreement, the bank had challenges with the Mexican affiliate.[21] The Department of Justice highlighted the Sinaloa, and the Norte del Valle Cartel was able to set up an account and then transmit wire transfers, move U.S. dollar banknotes across borders, or execute trade finance transactions without being detected, even with staggeringly large volumes.[22] Much of the problem centered on a lack of AML controls between affiliates in Mexico, Saudi Arabia, and operations in another 78 countries, many in high-risk AML jurisdictions.[23] HSBC was cited numerous times as being unable to close accounts, remediate customer files, or understand unusual customer patterns or behaviors between affiliates.

Within a banking group, and primarily related to large international financial institutions, there may be overseas subsidiaries, branches, joint venture partners, and offshore banking

---

[19] Bank of International Settlements. (2015, June 16). Bank statistics guide: Glossary - definition of affiliate. Retrieved from BIS international banking statistics: https://www.bis.org/statistics/bankstatsguide_glossary.pdf

[20] The paper uses the Bank of International Settlements definition of an affiliate as compared to the FINCEN 312 definition.

[21] U.S. Department of Justice. (2012, November 12). Deferred prosecution agreement - Statement of facts: Attachment A. Retrieved from https://www.justice.gov/sites/default/files/opa/legacy/2012/12/11/dpa-attachment-a.pdf - Page 11-14

[22] Ibid., pp. 3-8

[23] U.S. Senate Permanent Subcommittee on Investigation. (2012, July 17). U.S. Senate. Retrieved from U.S. vulnerabilities to money laundering, drugs, and terrorist financing: HSBC case history: https://www.hsgac.senate.gov/imo/media/doc/PSI%20REPORT-HSBC%20CASE%20HISTORY%20(9.6).pdf

centers. Typically, the management of affiliate accounts is an internal administrative process not given much oversight by senior management, because the business opens affiliate accounts without reservations or special consideration. For many financial institutions, this oversight translates to lending limits and capital restrictions, but seldom AML/CTF framework purposes alone.

Personal Liability for BSA Officers and MLROs

The rise of personal liability raises the specter that Bank Secretary Act (BSA) Offices or money laundering reporting officers (MLROs) will need to incorporate affiliates into their AML/CTF oversight and risk assessments. Currently, most financial institutions do not examine affiliate risk, or from the collective network of affiliates, as a source of AML/CTF risk. Instead, risk assessments focus on an entity's customers, products, services, and channels with little concern placed on internal parties. However, various enforcement actions have singled out affiliates as a source of risk. The U.S. Federal Financial Institutions Examination Council (FFIEC) manual directs BSA officers to have internal controls over banking operations without regard to geography.[24]

Inherent Risks of Affiliates

Correspondent banking elevates risks from customers, products, services, channels, and jurisdictions. The enterprise-wide risk assessment should identify the inherent risks, mitigation controls, and residual risks as part of the affiliate framework. Many institutions will focus on customers in high-risk jurisdictions or particular products, such as cash management services, international funds transfers, check clearing, payable through accounts, pouch activities, foreign exchange, sweep accounts, lending, and lines of credit.[25]

Some institutions may be tempted to treat affiliates similarly to third-party respondent banks. However, one should be cautious about using this approach, as this action will prompt additional and unnecessary administrative and legal documentation, especially with the presence of internal politically exposed persons (PEP). Leaders of financial institutions should create a

[24] Federal Financial Institutions Examination Council. (2014). Bank Secrecy Act: Anti-money laundering examination manual. Retrieved from: https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_047.htm
[25] Ibid.

separate category of internal PEP with a nuanced level of know-your-customer (KYC) and customer due diligence (CDD) that exempts duplicate documentation. It is unnecessary to get C-suite passports for ultimate beneficial owner (UBO) identification when this documentation resides in other functions, such as corporate secretaries or human resources. This process needs to use resources efficiently.

The risk around affiliates may remain inherently high, in part because many of the FCR controls are outward-oriented rather than inward. In the HSBC example, it was reported that the organization failed to conduct due diligence on HSBC Group affiliates, notably from its Mexican subsidiary.[26] This behavior leaves many organizations vulnerable to bad actors, able to transact between internal parties, often called "me-to-me accounts," that remain unmitigated. There may be different KYC standards or CDD processes. The transaction and sanction-monitoring scenarios may vary if different technologies are applied. Unfortunately, banks with overseas operations tend to be managed separately, with FCR controls complying with local regulation and little thought given to an integrated approach or to examining the account that is transacting between subsidiaries or branches.

Affiliate Risk Scoring

An affiliate can be judged across the separate control categories using the recently released Wolfsberg Due Diligence Questionnaire and supplementary materials.[27,28] In evaluating an affiliate's control framework, one can replace the [Yes/No] drop-down inputs with a scoring choice selection similar to the FATF mutual evaluation methodology. One issue remains: the lack of quantitative measures. While the questionnaire contains 13 sub-sections, removing three sections of a legal entity, products and services, and AML, CTF, and sanction risk assessment will make the approach simpler.

Similar to the FATF methodology, the inputs may be set to *highly effective*, *substantially effective*, *moderately effective*, and *low levels of effectiveness*. Additionally, the inputs may

[26] U.S. Department of Justice, op. cit., pp. Page 4-5
[27] Wolfsberg Group, op. cit.
[28] Wolfsberg Group. (2018). Correspondent banking due diligence questionnaire (CBDDQ) V1.2. Wolfsberg Group. Retrieved from: https://www.wolfsberg-principles.com/wolfsbergcb. The Wolfsberg Group's DDQ sections 3 to 13 can be utilized.

assign with numeric values, and the control categories can be weighted or use multipliers, depending on the approach. The output can be placed on a 40-point or 100-point scoring scale to evaluate an affiliate's controls. A highly effective affiliate should have a cumulative score in the top quartile.[29]

Red Flags

There are several types of red flags generated from internal entities. The following behaviors should prompt review:

- A high number of alerts concentrated on the same customer, types of customers, industries, or jurisdictions from a separate affiliate;
- A large number of suspicious activity reports (SARs) or suspicious transaction reports (STRs) written on the same customer, or types of customers or industries, or jurisdictions. Leaders of financial institutions should pay particular attention to affiliates located in free trade zones;
- Anonymous nested transactions, typically MT103s, where the customer names contain the word "bank," "money," or a similar word denoting a financial institution in the originator name, or field 50A;
- A high volume of deposits, use of remote deposit capture (RDC), or check clearing denominated in a currency other than that of the home country;
- An increasing or high volume of deposits, use of RDC, or check clearing used by nonresident or foreign customers;
- A high number of transactions between the same customer account located in different jurisdictions or a repeated pattern of transactional activity from high-tax jurisdictions to low-tax jurisdictions;
- The lack of responsiveness around requests for information;
- The transactional behavior occurs between a personal customer account and a corporate account located in different domains.

The affiliate management team may need to conduct investigations when an affiliate has an increasing or high volume of alerts, SAR, or STRs. Unlike Danske Bank, the function

[29] Highly effective scores may need to be calibrated to recognize the aggregated minimum scores.

requires to evaluate the causes across all currencies, products, services, and customers. Danske Bank was unable to divest the business interests related to a nonresident customer of its Estonia branch.[30]

Affiliate Governance Function

One way of addressing elevated FCR from the affiliate network is to create an affiliate governance function that incorporates the senior manager of all three lines of business to address the issue. The Affiliate Governance Forum, composed of elements from all three lines of defense, is a necessary function; however, audit's presence is as an observer to ensure unmitigated vulnerabilities and management self-identified issues are addressed in a timely manner. The senior manager regime is an approach that involves mapping roles and responsibilities within an organization[31] and is entirely consistent with managing affiliates.

In a more mature organization, the affiliate governance may be integrated into an existing governance structure; however, where there are deferred prosecution agreements in place, a financial institution may need to devote more attention to these risks. This action is especially true if the regulator has required immediate action.

Chief Executive Officer or General Manager Accountability Statements

An indispensable step is to put the proper incentives or disincentives in place. The chief executive officer (CEO) or general manager needs to have a job description that incorporates his or her responsibility for the overall FCR of that entity. While this seems self-evident to many, given the geographic scattering of entities, many senior managers may not be familiar with U.S. or UK laws. Also, an annual accountability statement may be necessary to remind the CEO of this responsibility.

Moreover, their job descriptions and performance evaluations should not prioritize business objectives or financial crime metrics. Compensation measures need to incorporate FCR inputs to ensure AML quality is not sacrificed to business objectives, as was observed in the

[30] Bruun & Hjejle, op. cit., p. 22
[31] Financial Conduct Authority. (2017, July 26). Senior Managers and Certification Regime: Banking. Retrieved from Financial Conduct Authority: https://www.fca.org.uk/firms/senior-managers-certification-regime/banking

Danske Bank example.[32] These FCR measures, such as alert backlogs and quality of SAR/STR filings, coupled with the enterprise-wide risk assessment, can reinforce compensation determinants. Many chief executives see their role as purely regarding revenue generation.

An approach for linking tone from the top with AML/CTF effectiveness in AML/CTF would be to score business heads. While one may avoid scoring CEOs directly, there is room to link executive accountability with AML/CTF performance. COOs and independent metrics would contribute to a performance measure having a 20% weight for AML/CTF effectiveness of members of the executive committee. A direct contributor to senior management performance may be a more effective method for driving a culture of compliance than the use of clawbacks.

The CEO exerts significant influence over an organization's culture; moreover, the CEO is responsible for ensuring that FCR is *not* exported to another entity and is required to take active steps to reduce risk. Many CEOs perceive that they are not strictly told they are responsible. Many compliance functions may feel pressure to exempt accounts from the review. However, as noted by U.S. regulators, the accountability of the clearing responsibility lies with that subsidiary, and CEOs or senior managers are often held accountable for the actions of other affiliates.

Affiliate Entity Management

The affiliate function is composed of the first line of business with affiliate relationship managers and a centralized second line compliance function within regions to share sensitive information and isolate areas of remediation. Three roles may exist within this framework. The affiliate relationship manager (ARM) works within the subsidiary or branch. The affiliate entity manager (AEM) operates from central or regional headquarters, while a remediation officer may be necessary to expedite remediation efforts of the weak entity.

---

[32] Danske Bank. (2018). "Report on the Danish FSA's supervision of Danske Bank as regards the Estonia case." Retrieved from: https://danskebank.com/-/media/danske-bank-com/pdf/investor-relations/fsa-statements/fsa-decision-re-danske-bank-3-may-2018-.-la=en.pdf
As noted on page 2 of the Danish FSA report, "35% of the profit in the branch in 2012 was generated by Russian customers, who made up 8% of the customer base."

Affiliate Relationship Manager

The role of the ARM, who is appointed by the CEO, is to facilitate requests between entities and the AEM. This function will handle any SWIFT account set-up, credit limits, or entity level management. As a note of caution, the ARM function should not be burdened with external customer relationships. The ARM will be the central contact point for facilitating the KYC/CDD requests that are housed in a central database. The affiliate KYC profiles should be housed in one central database to reduce administrative and bureaucratic processes. One core affiliate KYC profile should be produced without the need to build multiple versions if more than one currency is used. The ARM's central responsibility is to facilitate information requests and escalate controls issues.

Affiliate Entity Manager

The role of AEM is to manage affiliate entities. The function is the central control. One advantage is to centralize the Legal Entity Identifier (LEI)[33] management, the KYC/CDD processes, and have a centralized governance forum for escalating issues. It is also the function that conducts enhanced due diligence of troubled entities. At times, AEM will make due diligence calls or visits to relevant parties, depending on the severity of the issue, while at other times, they will direct assurance reviews or sample testing. When the issue is severe, it may require calls with the CEO or managing director in charge of the afflicted entity.

Establishing the affiliate function may involve centralizing regulatory reporting elements, credit reporting, and AML vulnerabilities together. Large financial institutions may have a greater need for this type of management; however, smaller regional banks may benefit, too. This entity will evaluate entity risk assessments against audit- and management-identified areas to assess their importance.

Remediation Officer

When remediation is required for more than six months, it may be necessary to appoint a remediation manager from senior management to initiate rehabilitation and provide oversight.

---

[33] LEI is a 20 alpha numeric code developed for each legal entity. Under International Organization for Standardization (ISO) 17442 standard, this code standardizes identification and clarifies relationships between legal entities involved in financial transactions.

Large financial institutions with branches and subsidiaries domiciled in non-U.S. jurisdictions may not view their accountability to the U.S. Bank Secrecy Act or UK Sanctions and Anti-Money Laundering Act 2018 in the same manner. This observation is especially true of Asian organizations, which may view AML/CTF differently. A remediation officer is added to the management team regarding areas needing remediation to address issues with customer KYC files, reducing alert backlogs, examining transactions, or sanction monitoring. The recent Société Générale's Consent Order is an example of the risk issues needing immediate attention.[34] The remediation officer's responsibility is to fix these types of problems. The remediation officer should report directly to the audit committee to ensure that activity is sustained and without interference from the involved parties.

The purpose of the affiliate management structure is to incentivize the business to embed effective processes while empowering FCR function to address the AML vulnerabilities promptly. As financial institutions vary, the role should reflect the organization's inherent risks and control framework. The management of affiliates should not be precisely like the management of external counterparties due to the conflicts of interest that arise when forced remediation is necessary.

Letters of Remediation

Unlike external relationships, an organization or clearing affiliate can require remediation actions from a branch or subsidiary. Hence, a letter of remediation issued from the CEO from the clearing affiliate upon another member may be a method to reduce financial crime risk. A typical letter of remediation may happen after an evaluation of an affiliate based on an enhanced due diligence review of the affiliate enterprise risk assessment and transactional activity and may incorporate interviews of the CEO and management team.

After an evaluation, the clearing affiliate may instruct the respondent banking affiliate to remediate customer accounts, KYC files, products and services, and FCR controls within a time-bound period, such as 45, 60, 90, and 180 days, banded by risk categories. These actions are

[34] New York State Department of Financial Services. (2018, November 19). Enforcement Actions - General. Retrieved from Consent Order to Société Générale SA and Société Générale, New York Branch - BSA/AML: https://www.dfs.ny.gov/reports_and_publications/press_releases/1811191 - Page 2

specifically focused on reducing financial crime risk and may impose a curtailment of services or require the exits of customers, products, and services. For example, if an affiliate is not addressing financial crime related to remote deposit capture around U.S. dollar check clearing, then the clearing affiliate may remove the service upon notice.

Notices to Affiliates

When transactional monitoring reveals issues, notices to affiliates are another form of notice to an affiliate by the affiliate management function. The action is often necessary when there are repeated SARs/ STRs filings. The note identifies customer or product vulnerabilities that require attention within a time-bound manner. The notices to affiliates will highlight the customer name, the infraction, the date, and the basis of concern.

The notice may notify a next block or pending block within 30 days to conform to local jurisdiction customer notices. It may require an entity to perform a due diligence review or to update KYC/CDD files to a set of higher standards. When an affiliate receives repeated FCR notices, there should be an escalation to the CEO followed by the governance forum.

Information Sharing Protocols

Banks with an international footprint will need to consider procedures for information sharing. Depending on the jurisdiction, it may be necessary to formalize the protocols between entities or to codify the policy into a group-wide sharing policy. FATF encourages information within organizations, but it should consider customer attributes, STR/SAR data, audit and assurance reports, enterprise risk assessments, due diligence reports, and management-identified issues aligned to Recommendation 18.[35] A group-wide protocol to enable the affiliate function to assess the consistency of controls is essential to the role. It is also the purpose of incorporating the second line of defense into the affiliate function.

Conclusions

Affiliate risk requires greater awareness and standards to result in more effective management of these entities. Currently, leaders of financial institutions are more concerned

[35] Financial Action Task Force. (2017). FATF guidance: Private sector information sharing. Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Private-Sector-Information-Sharing.pdf - Pages 7-11

about the outside threats than the hidden affiliate risks; however, affiliates may be a more significant source of correspondent banking danger. The following recommendations create standards and best practice regarding the management of affiliates as a separate function. Senior management must ensure that one subsidiary or affiliate is not exporting risk to another subsidiary or affiliate. The proposals outline a series of actions that may be required to bring an affiliate within risk appetite.

The management of correspondent banking governs affiliates with a similar standard of care, but may not be equal to third parties, and focused on ensuring that collective members are protected from both internal and external threats. As such, the responsibilities of the AML/CTF are shared between the first and the second lines of defense and melded into senior management governance. The framework requires the validation of trusted partners within the organizational configuration as an internal network of respondent banks with individual rights to initiate corrective actions and remediations.

Moreover, the affiliate entity management is a proactive governance framework that drives a partnership between senior management, the business, and the organization's risk management functions, including FCR. The leaders of successful organizations understand that affiliate management is not only about managing internal funding limits and clearing relationships, but also about ensuring that each affiliate maintains high standards and integrity within the corporate structure. The following recommendations are outlined to manage internal entities for their correspondent banking risks.

Recommendations

1. *Affiliate governance* should be established to prioritize AML/CTF consideration to parry business objectives and concerns. Without a function to evaluate the affiliate risk posed upon an organization, the first line of defense is likely to prioritize business interests or control risks.
2. *CEO accountability statements* inserted into the CEO's job description will align his or her performance review with overall organizational goals. Without an equalization of values, interest on revenues will always trump risks. When evaluating AML risk, which is

intertwined with outsized revenue streams, the CEO is the only counterweight to the business.

3. *Enterprise-wide AML standards* need to set AML standards and risk appetite across an entire organization. Standards are not confined to policies and procedures; they can also apply to technology and business practices. Due to the differences in development within countries, a financial institution needs to determine best practices. This decision-making requires that all three lines of defense are adequately incentivized.
4. *Affiliate function* is an essential element of governance. Relationship managers on the frontline need to be held accountable for the set-up of internal accounts with adequate supervision from the control function and senior management. For far too long, the businesses have treated affiliate management as purely an administrative function that involves creating entities, arranging internal limits, and moving payments without much regard for the internal and external risks.
5. *Letters of remediation* should be issued from one entity to another through the governance forum when one affiliate poses an unacceptable threat. This action is especially true when a memorandum requiring immediate attention is an issue, and prompt corrective action is necessary.
6. *Notices to affiliates* might be necessary should an affiliate continue to send customer transactions that generate elevated risk regarding alerts or SARs/STRs, and the clearing affiliate should provide the notice of account blocking. The remedy should be sent to the affiliate to conduct enhanced due diligence immediately on the account to ascertain the problem. A detailed write-up should be provided to the clearing affiliate's affiliate forum. An agreement on information sharing may need to be established, especially concerning SARs/STRs that are filed, and may need to be handled by the second line.
7. *Reporting* is essential, as affiliate data analytics and statistics need to be tracked to ensure that entities comply. This network awareness will highlight compliance gaps or vulnerabilities regarding senior-level engagement.

Final Thoughts

The affiliate entity management approach necessitates a common foundation shared across the broader FCR community. Large and small financial institutions can benefit from this operating approach that manages affiliate relationships, as well. This white paper makes a variety of practical recommendations; however, there are a variety of methods depending on organizations' operating models and governance culture.

Modern correspondent banking integrates a variety of products and services into a comprehensive set of processes that use both technology and people to exchange financial and nonfinancial information. Affiliate entity management is an essential part of the correspondent banking foundations. Correspondent banking and affiliate entity management are necessary for economic connectivity, but both aim to increase transparency and reduce FCRs exported to another entity.