Navigating Essential Anti-Money Laundering and Combating the Financing of Terrorism Requirements in Trade Finance:

A Guide for Respondent Banks

SEPTEMBER 2018 | VOL. 2

IN PARTNERSHIP WITH



IFC International Finance Corporation
WORLD BANK GROUP

Creating Markets, Creating Opportunities

Disclaimer

This brochure was developed to provide information about current compliance pertaining to anti-money laundering and combating the financing of terrorism (AML/CFT) in the trade finance space. This guide does not constitute legal or regulatory advice, nor guidance or advice regarding the preparation of policies and procedures relating to AML/CFT compliance. The practices and standards described in this guide may not be sufficient under applicable law or for another financial institution with which the user seeks to do business. Users of this guide are urged to seek their own advice with respect to AML/CFT standards applicable to them, as well as the practices and procedures that they implement with respect to AML/CFT compliance.

September 2018

Cover & Photo credits: World Bank Group Photo Collections

Navigating Essential Anti-Money Laundering and Combating the Financing of Terrorism Requirements in Trade Finance:

A Guide for Respondent Banks

SEPTEMBER 2018 | VOL. 2

IFC International Finance Corporation
WORLD BANK GROUP
Creating Markets, Creating Opportunities

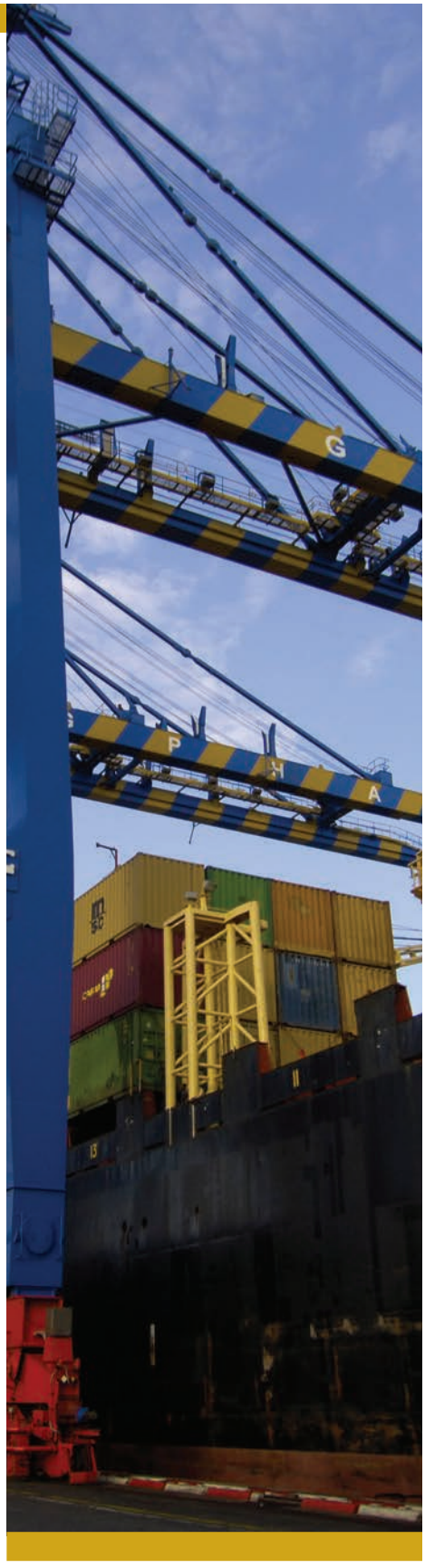
Contents

Acknowledgements

This updated version of "Anti-Money Laundering and Combating the Financing of Terrorism" (AML/CFT) brochure (vol. 2) was prepared by Makiko Toyoda, Susan Starnes, Robert Heffernan, Zeynep Ersel, Alexei Timofti, Ahmed Hanaa Eldin Mohamed, and Malik Rashid (KYC consultant) under the supervision of Hyung Ahn (Global Head, Trade and Commodities) at IFC (International Finance Corporation). It was reviewed by Ceri Wyn Lawley (Chief Compliance Officer), Yannick Stephant, and Lucas Diez Suarez (IFC) as well as Kuntay Celik (World Bank). IFC would like to thank the partners who provided insightful comments for this version, including Marc Auboin, Counsellor, World Trade Organization (WTO), Tod Burwell, President & Chief Executive Officer (CEO), Bankers Association for Finance and Trade (BAFT), and Olivier Paul, Head of Policy, International Chamber of Commerce (ICC). IFC is also grateful for the stakeholders who provided insight on current market developments, including African Export Import Bank, Society for Worldwide Interbank Financial Telecommunication (SWIFT), Thomson Reuters, Bankers Almanac, IHS Markit, and Global Legal Entity Identifier Foundation (GLEIF), among others. IFC is thankful for the opinions offered by issuing and confirming banks under IFC's Global Trade Finance Program (GTFP). Their input was critical to forming this publication. Lastly, IFC's GTFP Team would like to thank the International Development Association's (IDA) Private Sector Window (Creating Markets for Advisory Window) (CMAW), the Government of Japan, the Netherlands, and Sweden for funding IFC's trade advisory services, including this AML/CFT brochure, which is being used for IFC's trade finance training in IDA countries.



Introduction



As a global trade platform linking emerging market banks with international banks, IFC (International Finance Corporation) has supported over US$154 billion in emerging market trade through more than 560 banks in over 96 countries since the inception of its trade programs. IFC takes anti-money laundering and combating the financing of terrorism (AML/CFT) compliance seriously. This guide was prepared for the benefit of emerging market respondent banks, a group that relies on cross-border correspondent banking services to support the development of their clients and countries. AML/CFT regulations, Customer Due Diligence (CDD) processes, and procedures have developed to support global efforts to identify and address money laundering and the financing of terrorism. The publication presents an overview of AML/CFT and CDD requirement, particularly as it pertains to those involved with trade finance.

Strong risk management is essential to reduce the potential that the financial institution will be used to perpetrate financial crime. However, for some emerging market respondent banks, global AML/CFT efforts have contributed to correspondent banks' de-risking and other forms of correspondent bank network stress. The 2017 International Chamber of Commerce (ICC) survey[1] shows that nearly 30 percent of respondents say that financing the request of a trade was rejected as a result of AML/CFT-related concerns. In the same survey, nearly 80 percent of respondents agree (or strongly agree) that AML/CFT requirement is a barrier to servicing trade financing needs.

IFC's publication, "De-Risking and Other Challenges in the Emerging Market Financial Sector,"[2] notes that over 25 percent of 300-plus banks in over 90 emerging markets reported correspondent bank relationship losses. Beyond such losses, 72 percent of banks report that they face multiple exogenous challenges that reduce their provision of services. This immediately reduces market capacity to import what it needs to support business growth, including goods necessary for basic economic function and family survival.

1 International Chamber of Commerce, "Rethinking Trade & Finance," 2017, https://iccwbo.org/publication/2017-rethinking-trade-finance/
2 http://documents.worldbank.org/curated/en/895821510730571841/pdf/121275-WP-IFC-2017-Survey-on-Correspondent-Banking-in-EMs-PUBLIC.pdf

Increasing compliance costs, the specter of significant regulatory fines, and other factors related to AML/CFT compliance have led many global banks to reduce, exit or require more from trade finance relationships with banks in countries where the value of the relationships and markets no longer warrant the increasing cost and risk to maintain them. The multilateral community as well as several regional groups have become increasingly concerned that de-risking will pose significant and potentially systemic challenges to certain countries and markets. There are significant efforts underway to thoroughly understand and address this phenomenon.

For many emerging market respondent banks (and their customers), the increased expectation, complexity and fragmentation of regulatory and reporting requirements with respect to AML/CFT present unprecedented operational and system challenges. The small- and medium-sized enterprise (SME) clients of such respondent banks are most likely feeling the acute effects of de-risking. While many factors contributing to de-risking are beyond the control of respondent banks, this guide attempts to clarify important components of AML/CFT so that emerging market respondent banks can consider them while formulating and revising their strategy to secure, retain, and grow correspondent banking relationships.

To begin, this guide is intended to help clients identify the proper references for guidance, provide an overview of this guidance and begin to consider how to give effect to this guidance in their businesses and countries. This guide presents an overview of regulatory guidance on AML/CFT, including information and updates from the Financial Action Task Force (FATF) as well as the Basel Committee on Banking Supervision (BCBS) and other institutions. A separate overview on trade-based money laundering is included. The guide then presents global banks' perspectives related to CDD considerations in onboarding and maintaining bank customers in higher-risk jurisdictions. Finally, the guide considers third-party technology solutions that have arisen in response to the need to better manage the problem of rising AML/CFT-related costs. A full list of relevant resources is available in Appendix B; in addition to this guide, obtaining and carefully reviewing each document listed is recommended.

IFC has zero tolerance for trade-based money laundering and other financial crimes. This brochure is intended to be one of many resources that our partner banks can use to keep abreast of current AML/CFT developments as they relate to trade finance, and it complements IFC's training efforts on the same.

Hyung Ahn
Global Head
Trade and Commodities
International Finance Corporation

I. Market Perspectives on AML/CFT's Impact on Correspondent Banking Relationships

In performing due diligence, correspondent banks typically examine the strength of AML/CFT regulations in the country where their respondent bank is based. Publicly available disclosures[3] also impact CDD monitoring of a respondent bank. Global correspondent banks have significant information requirements that may exceed the information available in some jurisdictions. Thus, respondent banks are expected to invest the resources required to deliver information meeting global best practices of correspondent banks.

Money laundering is the processing of criminal proceeds to disguise their illegal origins and make them appear legitimate. Terrorism financing is the financing of terrorist acts, terrorists, and terrorist organizations with funds from a legal or illegal source. The Financial Action Task Force (FATF's) risk-based approach was designed to provide banks with greater flexibility in determining the most effective measures to identify and address money laundering/terrorist financing (ML/FT) risks.[4] This means that financial institutions or regulatory authorities are not specifically required to interpret and implement an AML/CFT approach in the same manner. Thus, due diligence requirements can vary from jurisdiction to jurisdiction and bank to bank. FATF's recommendations, including interpretive notes, and guidance papers help to clarify and guide implementation according to the principles.

Banks encounter two specific terms with respect to AML/CFT related customer assessment: Customer Due Diligence ("CDD") and Know Your Customer ("KYC"). Rising from the regulatory front, CDD was introduced by FATF in 2003 and further developed to include: identification and verification of customers, identification and verification of beneficial owners, understanding the nature and purpose of transactions, and monitoring the clients and their transactions on an ongoing basis.[5] Prior to 2003, the term "Know Your Customer" appeared to express the more general concept of gaining familiarity with your customer to assess their risk, and has been applied to AML/CFT risk. It is used widely by private sector companies and solutions providers as well as some governments, and does not have global regulatory consistency. Thus, either or both terms can be relevant, depending on a variety of factors.

Monitoring for ML/FT is performed at both the transaction level and the client level. Among correspondent banks, there are differences in how ML/FT risks are managed and how CDD is carried out on their respondent banks. Each bank has its own policies, risk appetites, and risk scenarios. Banks also face competing demands from regulators in multiple jurisdictions regarding how to achieve AML/CFT compliance. Even within one banking group, CDD processes and procedures may differ from one business line to another. Every bank (or every business line of a bank group) is responsible for any breach that arises in AML/CFT compliance. The inherently complex and hard-to-detect nature of

3 This is recognizing that some information to address AML/CFT compliance cannot and should not be publicly disclosed.

4 Financial Action Task Force (FATF), "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation – The FATF Recommendations," 2018, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

5 World Bank Group and Global Partnership for Financial Inclusion, "G20 Digital Identity Onboarding," 2018. https://www.gpfi.org/sites/default/files/documents/G20_Digital_Identity_Onboarding_WBG_OECD.pdf

trade-based money laundering (TBML) (as discussed in section IV) further adds to the challenge of achieving AML/CFT compliance.

Heightened regulatory scrutiny and fragmented regulatory interpretations, among others, have increased the cost of AML/CFT compliance requirements for correspondent banking. ICC's 2017 survey[6] states that maintaining a basic correspondent banking relationship has risen to €15,000 – €75,000. A Thomson Reuters survey indicates that financial institutions spend an average of US$60 million on KYC procedures (which include CDD).[7]

Beyond compliance costs, reputational risks associated with non-compliance of AML/CFT requirements are difficult to quantify, especially in an environment where there are more incidences of regulatory penalties being assessed if banks fail to comply with jurisdictional AML/CFT requirements. For example, even if a bank pays financial penalties related to AML/CFT related violations, its actual cost is larger when considering reputational damage. Moreover, if the risk of financial penalties is large enough, among other challenges, then AML/CFT compliance may translate into an operational risk problem since it necessitates banks' allocating more capital to provide for possible losses arising from the risk of having to pay penalties to regulators. Thus, confirming banks are particularly eager to avoid being complicit in financial crime.

There is a general consensus that trade-related AML/CFT compliance could be made more efficient if CDD best practices and other elements of AML/CFT were harmonized and clarified. There is also a near-consensus that AML/CFT compliance requirements can make trade finance more challenging.

What This Means for Your Bank

- Be aware: correspondent banks are facing much higher scrutiny for the relationships they have with your bank and others. Respondent banks need to invest in the necessary resources to meet best practices of correspondent banks' AML/CFT requirements.
- AML/CFT compliance requirements are becoming costly but are an essential investment to manage correspondent banking relationships.
- Be prepared: correspondent banks will ask for a significantly large amount of data, sometimes in new areas. Each correspondent bank may have differences in policies, information requirements, formats, reporting procedures.
- Plan for time and budget resource allocation to address each of your correspondent bank's requests. Bank staff need to be trained on an ongoing basis, particularly as regulatory requirements and applications continue to evolve.
- You are expected to implement a group-wide AML/CFT program, not just for select locations (branches or subsidiaries) of your bank. There must be an organizational culture of zero tolerance for ML/FT.
- Be responsive: correspondent banks typically seek to resolve potential "data flags," and timely responses to their requests will help them to manage compliance requirements more easily, thus improving your relationship.
- Your challenge is to maintain a sufficiently robust AML/CFT program so as to not be considered "risky" by your correspondents. If you are considered risky because your risk culture, systems, processes, decision making, and other factors are insufficient, you will be subject to more difficult and costly CDD procedures from correspondent banks, and may be putting those relationships at risk.
- Having the reputation of being a responsive respondent bank with market knowledge regarding ML/FT and an effective AML/CFT regime will help your standing with your network of correspondent banks.

6 International Chamber of Commerce, "2017 Rethinking Trade & Finance," 2017, https://iccwbo.org/publication/2017-rethinking-trade-finance/
7 https://blogs.thomsonreuters.com/financial-risk/investment-management/kyc-aml-landscape-2017/

II. Overview of Recommendations and Standards for AML/CFT

The Financial Action Task Force's (FATF) recommendations are intended to serve as the international standards for combating money laundering and the financing of terrorism. FATF states that their recommendations set out a comprehensive and consistent framework of measures that countries should implement in order to combat ML/FT, and FATF has continued to publish updates and clarifications related to these recommendations.

Last updated in February 2018, FATF's current definitions of the 40 recommendations[8] are categorized according to seven areas:

- AML/CFT Policies and Coordination
- Money Laundering and Confiscation
- Terrorist Financing and Financing of Proliferation
- Preventive Measures
- Transparency and Beneficial Ownership of Legal Persons and Arrangements
- Powers and Responsibilities of Competent Authorities and Other Institutional Measures
- International Cooperation

The mechanism for implementing FATF's recommendations will vary from jurisdiction to jurisdiction, but the recommendations are intended to harmonize the principles and standards that underpin the implementation of AML/CFT measures, while supporting flexibility within and among banks, countries, and other stakeholders for interpreting and applying FATF's guidance. This approach is pragmatic in that it allows a bank to take mitigation measures that are proportionate to the ML/FT risks and revenue opportunities that they see with a respondent bank and the country in which it operates; it also allows banks to continue to adapt as the AML/CFT landscape evolves.

The full table of recommendations is attached in the appendix. Each of the enforcement areas are further defined below.

- AML/CFT Policies and Coordination

Countries and banks should identify, assess, and understand the money laundering and terrorist financing risks that they face. Policies, processes and other measures that are commensurate with the identified risks need to be implemented to prevent or mitigate ML/FT. Such a risk-based approach serves as the essential foundation to optimal allocation of resources for implementing a country's AML/CFT regime. Countries should designate an authority or empower a group

8 Financial Action Task Force (FATF), "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation – The FATF Recommendations," 2018, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

of competent authorities for effective enforcement of AML/CFT policies. Effective enforcement of AML/CFT policies also requires proper cooperation, coordination, and information sharing among enforcement authorities and banks.

- Money Laundering and Confiscation/Terrorist Financing and Financing of Proliferation

Countries should criminalize money laundering and terrorist financing on the basis of international conventions.[9] In enforcing policies against money laundering, competent authorities should be enabled to freeze or seize and confiscate any proceeds and assets that have been (or are intended to be) laundered or used (or to be used) for acts of terrorism.

- Preventive Measures

Preventative measures are an important component of FATF's recommendations. All financial groups (including all branches and majority-owned subsidiaries) must implement group-wide AML/CFT regimes, including policies and procedures for sharing information within the group for AML/CFT purposes. CDD needs to be undertaken at onboarding and performed on an ongoing basis, including adequate verification of customer identity and beneficial owners. Wolfsberg's 2018 Correspondent Banking Due Diligence Questionnaire[10] included as many as 16 questions on ownership. The Questionnaire is designed to help correspondent banks assess their respondent banks' capacity for CDD and other AML/CFT efforts. A key set of questions in this category pertains to the details of the ultimate shareholders with sizable stakes in the respondent bank. Correspondent banks need to be able to unpack ownership stakes of 10 percent or higher to identify the ultimate shareholders.

Banks also need to be able to identify PEPs (both from outside their countries and within their borders). Due diligence on politically exposed persons should require additional due diligence and surveillance to ascertain whether the bank is at risk of aiding in financial crime. Assessments of money laundering or terrorist financing risks and the implementation of appropriate measures to manage those risks are needed during the development of new products, business practices, and technologies.

Correspondent banks need to perform an assessment of the capacity and strength of the respondent bank's AML/CFT regime. For correspondent banking services that allow "payable-through accounts," the respondent bank needs to demonstrate that it conducts satisfactory due diligence on its customers and that it is able to provide such information upon request to the correspondent bank. Respondent banks in higher-risk countries should expect additional due diligence and monitoring requirements by their correspondent banks.

Wire transfers throughout the payment chain should reflect accurate and adequate information for originator and beneficiaries. Financial institutions are responsible for freezing and prohibiting transactions with designated persons and entities as set out in the United Nations (UN) resolutions on the prevention and suppression of terrorism and terrorist financing.[11] If a bank has grounds to suspect that client funds are proceeds of criminal activity, it should report to the country's financial intelligence unit. All records should be maintained for at least five years. To support a country's effective enforcement of AML/CFT policies, banks should be protected from any legal liabilities that may arise from confidential sharing of information with regulators over suspicious transactions.

9 Terrorist Financing Convention, Vienna Convention, and Palermo Convention, among other international conventions.
10 Wolfsberg Group, "Wolfsberg Group Correspondent Banking Due Diligence Questionnaire (CBDDQ), Version1.2," 2018, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_CBDDQ_220218_v1.2.pdf
11 http://www.un.org/law/cod/finterr.htm

- Transparency and Beneficial Ownership of Legal Persons and Arrangements

Countries and banks should take measures to prevent the misuse of legal arrangements for money laundering or terrorist financing. Information on legal persons and beneficial ownership maintained by a bank needs to be adequate, accurate and accessible to the relevant authorities that enforce AML/CFT policies. Sufficient controls must be in place to prevent the misuse of legal persons for financial crime.

- Powers and Responsibilities of Competent Authorities and Other Institutional Measures

The regulatory and supervisory measures (including the authority to conduct inspections) that apply for prudential purposes should apply in a similar manner for AML/CFT purposes. Banks need to be able to readily produce information that is relevant to the bank supervisors for effective surveillance over financial crimes. Banks that are not compliant with AML/CFT policies should be subject to a range of disciplinary and financial sanctions by bank supervisors.

- International Cooperation

There are several international conventions governing financial crime that countries are implementing, and these conventions are expected to evolve going forward. Financial crimes are often cross-border in nature; therefore, the effectiveness of combating money laundering and financing of terrorism is highly dependent on international cooperation between countries and banks. Countries are expected to cooperate in the enforcement and investigations of financial crime without undue restrictions on cross-border mutual legal assistance. Such cooperation needs to cover the freezing and confiscation of assets, extradition, and others.

Further Clarifications to the Recommendations from FATF and Basel

The flexibility in adapting and interpreting AML/CFT regulations has contributed to less consistency and clarity in inter-bank application, as well as to potentially higher KYC costs for some banks. This may inhibit correspondent banking and trade through the formal (transparent) financial sector channels. FATF recognizes that combating financial crime should not raise barriers to trade, and issued a supplemental guidance specific to correspondent banking services in October 2016,[12] which seeks to clarify guidance on "Know your customers' customers (KYCC)."

Some correspondent banks interpreted FATF's original guidance on correspondent banking (recommendations numbers 10 and 13) to mean that correspondent banks are required to carry out CDD on the customers of respondent banks. FATF's October 2016 guidance states that this is not the case; rather, the correspondent bank has the responsibility to regularly monitor the respondent bank's risk profile and take risk mitigation measures as and when needed, which aligns with FATF recommendation's underlying principle of taking a risk-based approach to AML/CFT.

While FATF does not require KYCC, the October 2016 guidance is quite prescriptive in a correspondent bank's responsibilities regarding due diligence and ongoing monitoring of respondent bank customers. FATF expects a higher burden of risk due diligence and monitoring for respondent banks considered to be high risk. Even if KYCC is not an explicit requirement, correspondent services that involve nested relationships and payable-through accounts require additional scrutiny (both at onboarding and during monitoring) from the correspondent banks if the respondent bank is based in a high-risk country. It is critical that these respondent banks have robust AML/CFT capacity in order to gain the confidence of correspondent bank counterparties both at onboarding and monitoring. An ongoing open dialog between correspondent and respondent banks is important for managing the correspondent banking relationship.

In June 2017, the Basel Committee on Banking Supervision (BCBS) published its own guidelines on managing ML/FT risks, including an annex dedicated to correspondent banking.[13] The BCBS guidelines are intended to be consistent with and supplement the goals and objectives of FATF, as they fully embody FATF recommendations (including the risk-based approach), as well as the Committee's principles on ML/FT risk management. The BCBS guidelines' dedicated section on correspondent banking also echo FATF's nuanced position on KYCC: correspondent banks generally are not required to conduct due diligence on respondent banks' customers, however, correspondent banking services with respondent banks in high-risk jurisdictions will naturally be recommended to conduct higher levels of due diligence and ongoing information requirements about the latter's customers and their activity. Given the array of regulatory interpretations, correspondent banks see it as necessary to fully comprehend and be comfortable with respondent banks' culture, processes, oversight and data.

Such high-risk countries are reviewed by correspondent banks regularly on their capacity to combat money laundering and financing of terrorism, and the risks these jurisdictions pose to the international financial system. These country-specific analyses serve as inputs to CDD procedures carried out by correspondent banks. FATF, along with its FATF-style Regional Bodies ("FSRB"s), identifies countries and jurisdictions with weak AML/CFT measures and works with them to address such deficiencies The Basel Institute on Governance also publishes the AML Index[14] annually for over 140 countries.

From the perspective of respondent banks, both the FATF and BCBS publications cited here should help them to anticipate correspondent banks' requirements for due diligence and ongoing monitoring for AML/CFT risks. Ongoing monitoring, as described in the BCBS guidelines, is an essential part of ML/FT risk management. Banks must understandwhat constitutes normal and reasonable banking activities of each of their customers in order to detect

12 FATF, "FATF Guidance on Correspondent Banking Services," October 2016. http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

13 Basel Committee on Banking Supervision (BCBS), "Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism," June 2017, https://www.bis.org/bcbs/publ/d405.pdf

14 https://index.baselgovernance.org/

suspicious transactions. All banks must have systems in place to detect such activity, as well as related processes to identify, investigate, and report them.

In addition to the FATF and BCBS guidelines, banks must also follow developments from regulators responsible for regulatory oversight of major correspondent banks. For example, the European Commission has introduced AML Directives to improve enforcement of its AML/CFT laws. The A fifth directive became effective in 2018.[15] The United States (U.S.) Treasury Department's Financial Crimes Enforcement Network (FinCEN) also made new requirements for customer due diligence effective in 2018.

Summary of Essential Points

- FATF's 40 recommendations serve as international standards for combating money laundering and financing of terrorism.
- FATF's recommendations explicitly require the criminalization of ML/FT.
- Of the seven areas of enforcement, the core recommendations pertaining to preventive measures are the most prescriptive to a bank's day-to-day operations and risk management.
- In addition to banks, the recommendations impose heavy responsibilities on countries to manage financial crime risks.
- Risk-based principles apply in the implementation and enforcement of AML/CFT policies—measures taken need to be proportionate to the risks identified.
- Combating money laundering and financing of terrorism require cross-border information sharing and cooperation by regulators and banks.
- Respondent banks in high-risk jurisdictions should have robust AML/CFT regimes to manage heightened scrutiny from their correspondent banks.

What This Means for Your Bank

- You will be expected to understand and apply the risk-based approach and have clear and specific conversations with your correspondent banks and regulators as to how you are performing your own risk assessments.
- You need to be able to articulate the specific ML/FT risks in your markets and implement appropriate steps to manage them. Different markets have different areas of risk, and your ability to manage them up to international standards will demonstrate market wisdom. All countries have or are developing AML/CFT risk assessment procedures which would connect with local banks' efforts, ensuring that you have identified the right contacts for collaboration is essential.
- Your relationships with regulators and enforcement authorities would support the strength of your AML/CFT. Establishing a functional channel of communication and engagement with each regulatory entity with regard to ML/FT could position your bank as a leader in combating ML/FT in the local market.
- You would need to check into jurisdictional legal allowances/requirements for cross-entity information sharing to determine where you may have opportunities to learn more about your clients, and where there may be barriers.
- It is important to know your customers thoroughly: who they are (robust identity verification), where they live, who they work for, and from where their assets originate. This is important to avoid being complicit to financial crime.
- Knowing your customer does not end after onboarding; you are expected to collect and maintain up-to-date information on each one of them, and monitor their transactions. Beneficial ownership needs to be unpacked to identify precisely the ultimate beneficial owners.
- Onboarding and ongoing due diligence entails understanding the transactions that constitute normal banking activities for each customer and having methodologies for flagging transactions that fall outside of that norm.
- If it has not done so already, your jurisdiction may move toward encouraging cross-border information sharing on potential ML/TF crimes. Over time, your bank should work towards being operationally ready to meet such a requirement.
- Your bank's AML/CFT regime needs to have systems, processes, and procedures that are effective in managing ML/FT risks and meeting the requirements of regulators and correspondent banks. Balancing this effort with budgetary investment constraints will be an important challenge to overcome. However, these efforts may also give rise to interesting market opportunities for new segments as your bank continues to improve its risk identification capacity.

15 https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/anti-money-laundering-and-counter-terrorist-financing_en

III. Wolfsberg Principles and Related Initiatives

Many national regulators are continuing to evolve their application of the risk-based approach, clarifying and developing their national AML/CFT strategies to conform to international standards. Industry initiatives are also responding to the growing challenges of customer due diligence. The Wolfsberg Group, an association of thirteen global banks, has contributed to the development of core principles, best practices, and other frameworks for more effective management of financial crime risks by financial institutions, globally. Presented below is a summary of five recent Wolfsberg Group's publications for the trade finance community. The paper on trade finance principles is a collaboration between the Wolfsberg Group, ICC, and the Bankers Association for Finance and Trade ("BAFT").

- Correspondent Banking Due Diligence Questionnaire (2018)[16]

The 2018 Correspondent Banking Due Diligence Questionnaire (CBDDQ) is part of an effort to standardize minimum KYC information requirements (for both onboarding and monitoring) for respondent banks and reduce any additional requirements. The questionnaire contains 110 questions over 17 pages, which is substantially longer and more detailed from the prior template, published in 2008. Table 1 lists all due diligence categories covered in the questionnaire and the nature of questions asked in each.

Some respondent banks completing this questionnaire may find it resource-intensive. Respondent banks need to proactively update their correspondent banks regularly on any change that the latter would deem material.

- Anti-Money Laundering Principles for Correspondent Banking (2014)[17]

These principles reflect FATF's 40 recommendations, which should serve as the basis of any financial institution's AML/CFT regime. All respondent banks are subjected to the appropriate due diligence to satisfy a correspondent bank that it is comfortable conducting business with them. These principles for correspondent banking relationships echo the risk-based approach that should be taken in customer due diligence and in the ongoing monitoring of the banks' relationship. Regarding AML/CFT principles around correspondent banking, the October 2016 FATF paper and the June 2017 BCBS guidelines are more current and prescriptive on AML/CFT principles governing correspondent banking than the 2014 Wolfsberg paper.

16 Wolfsberg Group, "Wolfsberg Group Correspondent Banking Due Diligence Questionnaire (CBDDQ), Version1.2," 2018, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_CBDDQ_220218_v1.2.pdf

17 Wolfsberg Group, "Anti-Money Laundering Principles for Correspondent Banking," 2014, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/8.%20Wolfsberg-Correspondent-Banking-Principles-2014.pdf

Table 1: Wolfsberg Correspondent Banking Due Diligence Questionnaire Categories

	Category	Nature of Questions
1.	Entity and Ownership	Questions aim to understand who/what the customer is, including details on ultimate beneficial owners
2.	Products and Services	Questions on correspondent banking, followed by related questions as to whether the respondent offers certain products and services
3.	AML/CFT and Sanctions Program	Information for the correspondent bank to assess the adequacy of overall control frameworks in these two areas
4.	Anti-Bribery and Corruption	
5.	Policies and Procedures	Further details on what is included in the respondent bank's policies and procedures
6.	AML, CFT, and Sanctions Risk Assessment	Extent of coverage of the respondent bank's enterprise-wide risk assessment in the areas of AML/CFT
7.	KYC, CDD, and EDD	Details of a respondent bank's due diligence process for its customers
8.	Monitoring and Reporting	Details on how the respondent bank monitors its customers and their transaction activities; how the bank reviews, escalates and repots alerts from monitoring systems
9.	Payment Transparency	Controls in place to accurately maintain the required data for originators and beneficiaries; processes in place to handle and respond to requests for information (RFIs) (Adhering to Wolfsberg Group payment transparency standards)
10.	Sanctions	Policies, procedures, and processes in place to ensure compliance with international sanctions programs to identify and interdict circumvention attempts
11.	Training and Education	Extent and scope of how all respondent bank staff are trained to understand financial crime risks, to identify suspicious activity, transactions, circumstances, scenarios, and to escalate concerns
12.	Quality Assurance/ Compliance Testing	Processes in place to test compliance with the respondent bank's policy and procedural requirements such that both first- and second-line controls are tested and enhanced continuously
13.	Audit	Type of audit mechanism deployed, what is covered in terms of assessing financial crime compliance related requirements, as well as how findings are tracked and monitored

- Wolfsberg Guidance on Society for Worldwide Interbank Financial Telecommunication (SWIFT) Relationship Management Application (RMA) Due Diligence (2016)[18]

RMA is a messaging capability that authorizes communications between members of the SWIFT network. It replaces the prior mechanism, the Bilateral Key Exchange (BKE). The 2016 Wolfsberg Guidance provides recommendations for managing non-customer RMAs. A non-customer RMA is generally created in network bank arrangements, when there is a request that the bank, in support of a customer's business, exchange SWIFT messages with a non-customer bank. For example, regarding a letter of credit in trade finance, a bank may need to exchange messages with other banks with which there is no direct payment relationship (i.e. a non-customer). Alternatively, in cash management, a bank may need to relay payment instructions from a corporate customer to a third-party bank.

Arrangements for establishing and approving RMAs need to be strong enough to avoid their being used as a tool for financial crimes. The following are minimum due diligence and ongoing monitoring procedures recommended by Wolfsberg for such RMAs; however, considering the risk-based principles articulated by FATF, these minimum standards should not be seen as exhaustive for each non-customer RMA:

1. Collect name and address information.
2. Conduct sanctions screening against relevant sanctions list(s), as appropriate.

18 Wolfsberg Group, "Guidance on SWIFT Relationship Management Application (RMA) Due Diligence," 2016, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/7.%20SWIFT-RMA-Due-Diligence.pdf

3. Conduct a review against internal red flag lists. In this context, red flag lists refer to lists that banks may maintain to manage or monitor transactions/relationships with particular entities. These are generally based on a variety of factors including, but not limited to, prior unusual transaction history and negative media reports.
4. Evaluate risks of the potential RMA based on the above information to identify whether a bank may require further review, based on internal risk tolerance.
5. Conduct periodic reviews of message volumes sent to/received from non-customer RMAs to determine if volumes and/or message types warrant additional due diligence due to significant changes in usage or cancellation due to non-usage conduct sanctions and internal red flag screening periodically in accordance with internal screening standards. Periodic screening should be done against names added since the previous periodic review.
6. If a bank has not historically screened RMAs against sanctions and red flag lists, a review of the existing files should be conducted within a reasonable time period.

- Trade Finance Principles (2017; jointly drafted with ICC and BAFT)[19]

Banks should determine their own compliance requirements for trade finance using a risk-based approach, as stated in FATF's 40 recommendations across seven categories (as discussed earlier). The 2017 Wolfsberg paper recognizes the challenges facing trade finance banks in managing risks arising from financial crimes. In reviewing each trade transaction for fraud, sanctions, and unusual or suspicious activities, transactions are often complex and largely paper-based, and involve a large number of parties. While some areas of risk management in trade finance may be automated, manual controls will remain relevant for every bank. The complex, paper-based documentation behind every transaction requires manual scrutiny of a large amount of information about the parties and goods being transferred. Each bank will need to configure their own transaction monitoring programs that are consistent with the business risks and AML/CFT compliance requirements.

Trade finance banks are reminded that the standard three lines of defense in risk management apply to managing financial crime risks – business operations, oversight, and internal audit. Escalation of a trade transaction means the filing of an "unusual transaction report" or a "suspicious activity report" with the relevant regulatory authorities. The table below presents specific examples of how trade-based money laundering (TBML) risks may materialize across some or all of the following product areas: documentary credits, bills for collection, and guarantees/stand-by letters of credit.

19 Wolfsberg Group, "Wolfsberg Group, ICC and BAFT Trade Finance Principles," 2017, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/comment-letters/6.%20Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf

Table 2: Examples of Red Flags in ICC/BAFT Trade Finance Principles[20]

Red Flag Types	When: Pre or post transaction
Deal Structures • Beyond capacity and or substance of customer • Improbable goods, origins, quantities, destination • Unusual complexity and or unconventional use of financial products	PRE or POST
Goods • Applicable import or export controls regulations may not be complied with	PRE – as part of onboarding customer due diligence
• Blatant anomalies in value versus quantity • Totally out of line with customer's known business	PRE or POST
Countries and Names • On the sanctions or terrorist list	PRE
Countries • On the bank's high-risk list • Any attempt to disguise or circumvent countries involved in the actual trade	PRE or POST
Claims and Payment Instructions • Illogical • Last minute changes to payment instructions • Claims made within a short time after issuance • Continuous claims under various guarantee instruments • Claim pressure tactics	PRE or POST
Repayment Arrangements • Third parties are funding or partly funding the Documentary Collection (DC) value (just in time account credits to the settlement account)	POST
DC Patterns • Constantly amended or extended • Routinely cancelled or unutilized	POST
DC Parties • Connected applicant and beneficiary • Applicant documentation controls payment	PRE or POST
Bills for Collection (BC) Parties • Connected Drawer or Drawee	PRE or POST
Discrepancies in Documents • Goods descriptions differ significantly • Especially invoice versus shipping documents • Unexplained third parties	PRE or POST
Discrepancies Waived • Advance waivers provided • Absence of required transport documents • Significantly overdrawn DC (tolerance allowed by standard practice)	PRE or POST

Relying on FATF's risk-based approach, the above table should inform how a bank should implement controls to detect risks based on its role in each transaction type. This list of red flags should be reviewed along with what FATF has published since 2006 across three publications (as presented in section V on trade- based money laundering).

20 http://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paper.pdf

- Payment Transparency Standards (2017)[21]

These standards support FATF's recommendations on preventive measures, especially on information transparency of wire transfers. They apply to all cross-border transactions regardless of value. For every payment, the Wolfsberg standards outline transparency responsibilities for originating financial institutions (FIs), intermediary FIs, and beneficiary FIs.

Table 3: Transparency Responsibilities for Wire Transfers outlined in the Wolfsberg Payment Transparency Standards

Type of Bank	Responsibilities
Originating Bank	• Verification, identification and due diligence of customer, as well as related record keeping in line with all the applicable regulations • Accuracy and completeness of information in the payment message concerning the originating party • Maintaining adequate records that permit the reconstruction of messages if required • Ensuring that messages contain all required information, as well as any other information stipulated by applicable regulations and guidance • Ensuring the correct use of payment messages to facilitate identification of payment information by all banks in the payment process • Including detailed information on the beneficiary party[20]
Intermediary Bank	• Passing on complete information that is received within payment messages to the next FI in the payment chain • Retaining a record of all the information received from the Originating FI or the Intermediary FI immediately upstream in the payment chain • Monitoring for compliance with FATF Recommendation 16 and implementing relevant regulation • Risk-based policies and procedures to determine when to execute, reject or suspend a payment and take appropriate escalation
Beneficiary Bank	• Verification, identification and due diligence of its customer (the beneficiary party), as well as related record keeping • Monitoring for compliance with the relevant regulations • Risk-based policies and procedures to determine when to execute, reject or suspend a payment and take appropriate escalation

Financial institutions should not omit, delete or alter information in payment messages for the purpose of avoiding detection in the payment process. Subject to all applicable laws, financial institutions should cooperate as fully as practicable with other financial institutions in the payment process when requested to provide information about the parties involved.

21 Wolfsberg Group, "Wolfsberg Group Payment Transparency Standards," 2017, https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf

22 This Wolfsberg paper has more technical instructions on how to fill out a beneficiary party's information.

Summary of Essential Points

- The Wolfsberg Group's publications on principles, best practices, and other frameworks are intended to introduce efficiencies to customer due diligence in correspondent banking relationships.
- The 2018 Correspondent Banking Due Diligence Questionnaire is a significant recent development. Respondent banks that lack well-defined processes to manage due diligence and monitoring by correspondent banks may find it useful to adopt the questionnaire.
- Wolfsberg's CBDDQ may also be integrated into the KYC utility that a respondent bank chooses to adopt (as discussed later in this publication).

What This Means for Your Bank

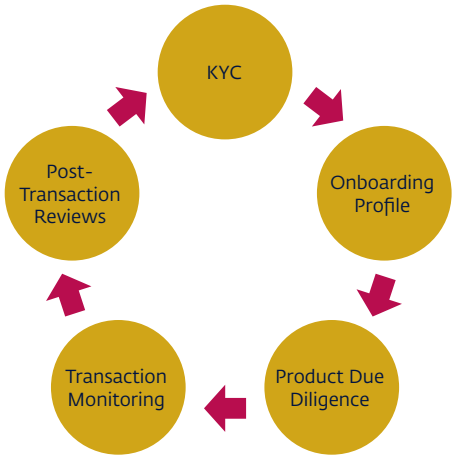
- To the extent that you have not done so, your bank should integrate Wolfsberg's 2018 CBDDQ as the foundation for the institution's AML/CFT readiness in managing correspondent banking relationships.
- One-time completion of the questionnaire is not sufficient. Banks need to regularly update the questionnaire's standard data requirements and communicate them to the correspondent banks.
- After operationalizing the regular use of CBDDQ, be more proactive in communicating with correspondent banks about your AML/CFT capacities. This could occur through an in-depth presentation or an in-person sight visit by correspondent banks. This communication should be part of your effort to elevate the level of comfort that the latter has in your bank.
- Consider adopting the use of a KYC utility (described below) that already has Wolfsberg's CBDDQ embedded in it.
- The CBDDQ can also serve as a blueprint for how your bank carries out CDD on your own customers, which may help you to exceed the minimum AML/CFT requirements in some jurisdictions.
- Wolfsberg principles, best practices, and frameworks should inform how your bank carries out ongoing staff training on ML/FT. These should also inform your bank's operational risk reviews to identify weak areas within your AML/CFT regime.
- Confirm how effective your bank is in detecting trade-based money laundering (TBML) red flags, and determine how to strengthen your processes if needed. More TBML red flags are listed later in this document.

IV. Trade-Based Money Laundering

Beyond the use of the financial system and physical movement of money (e.g. cash couriers), financial crimes also occur through trade. The international trade system has a wide range of risks and vulnerabilities that can be targeted for financial crime, which includes, among others, the large transaction sizes relative to some other forms such as remittances or consumer debt. The basic techniques of trade-based money laundering (TBML) include:

- over- and under-invoicing of goods and services;
- multiple invoicing of goods and services;
- over- and under-shipments of goods and services; and
- falsely described goods and services.

Exhibit 1: Monitoring Documentary Trade Transactions[23]



Documentary Red-Flags

- Discrepancy review
- Vessel checks
- Goods description/Dual-use screening
- Payment terms
- Shipping ports
- Fraudulent documents

Detection of TBML may be more difficult since volumes of trade flows are massive and because TBML can take complicated forms. Greater capacity building and more effective cooperation on information sharing is especially necessary for the prevention of TBML. FATF has published two separate guidance papers to address concerns related to TBML. A related paper was published by the Asia/Pacific Group (APG) on Money Laundering, which is a FATF-style regional body for the Asia-Pacific region.

23 Diagram presented by Tod Burwell, President and CEO, BAFT, during ICC Annual Meeting in April 2018.

- Trade based money laundering (2006)[24]
- Best Practices on Trade Based Money Laundering (2008)[25]
- APG Typology Report on Trade Based Money Laundering (2012)[26]

FATF sets the industry definition for trade-based money laundering, which is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. This definition was set in a 2006 paper and has been used in the two subsequent publications from 2008 and 2012. The list below is a consolidated set of red flag indicators of trade-based money laundering that are discussed in the three papers listed above:

- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value
- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities
- The type of commodity being shipped is designated as "high risk" for money laundering activities[27]
- The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities
- The shipment does not make economic sense[28]
- The commodity is shipped to or from a jurisdiction designated as "high risk" for money laundering activities
- The commodity is transshipped through one or more jurisdictions for no apparent economic reason
- The method of payment appears inconsistent with the risk characteristics of the transaction[29]
- The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction
- The transaction involves the use of repeatedly amended or frequently extended letters of credit
- The transaction involves the use of front (or shell) companies
- Unusual deposits of cash or negotiable instruments in round denominations
- Inward remittances in multiple accounts and payments made from multiple accounts for trade transaction of same business entity. Such use of multiple accounts for foreign exchange flows may indicate the possibility of TBML
- In the case of merchanting trade, the trade finance mechanism is not in place for both legs of the trade. For example, if a letter of credit is provided for only the import leg of the transaction and not for the export leg, this indicates a possibility of TBML
- Presence of free trade zones, or special economic zones
- Circuitous route of shipment, financial transaction, or order for the goods is placed by entities in countries other than the jurisdiction of the stated end user

24 FATF, "Trade-Based Money Laundering," June 23, 2006, http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf
25 FATF, "Best Practices on Trade Based Money Laundering, June 20, 2008, http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf
26 Asia/Pacific Group on Money Laundering, "APG Typology Report on Trade Based Money Laundering, " July 20, 2012, http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf
27 For example, high-value, low-volume goods (e.g. consumer electronics), which have high turnover rates and present valuation difficulties.
28 For example, the use of a 40-foot container to transport a small amount of relatively low-value goods.
29 For example, the use of an advance payment for a shipment from a new supplier in a high-risk country.

- Transaction involves shipment of goods inconsistent with normal geographic trade patterns
- Numerous companies set up by seemingly unrelated people (proxies) are found to be controlled by the same group of people
- Trade transaction is a related party transaction

The APG publication also lists descriptions of the vulnerabilities related to each trade finance instrument.

Table 4: Vulnerability of Trade Finance Instruments as identified in the APG Typology Report on Trade Based Money Laundering[30]

Instrument of Trade Finance	Their Vulnerability
Bills of Exchange	• If the parties are complicit, this may be undertaken and paid for without any form of due diligence by an intermediary in the supply chain • Phantom trades may arise from unrealistic timeframes or unrealistically short supply chains
Countertrade	• Exchange ratios for the goods may be determined by negotiation rather than by market
Documentary Credit	• Misrepresentation of price, quantity, and quality of underlying goods • Paper trail may be used to disguise illegal proceeds
Open Account Facilities	• Possible disconnect between the movement of underlying trade and the money used to finance it. • Payments against these facilities may not necessarily be undertaken through an international fun transfer instruction (IFTI) or SWIFT
Factoring	• Factors may be left with losses if the underlying trade is a sham
Forfaiting	• Since the underling instrument can be sold on secondary markets, this provides a money launderer with an enhanced mechanism to move value
Pre-Shipment Finance	• Provides money launderer with the ability to engage a third party in another jurisdiction
Post-Shipment Finance	• Cash is usually supplied at the time of sale
Buyer's Credit	• Financing an importer in a foreign jurisdiction widens the scope for TBML
Supplier's Credit	• Financing arrangement may not involve a financial institution

30 Asia/Pacific Group on Money Laundering, "APG Typology Report on Trade Based Money Laundering, " July 20, 2012, http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

To supplement the above list of FATF red flags and APG's analysis of vulnerabilities of each instrument, BAFT[31] has published its own table which maps BAFT's red flags to three different payment types:

Table 5: BAFT Red Flags in "Combatting Trade Based Money Laundering: Rethinking the Approach"

	BAFT red flags	Payments	Open Account Trade Payments	Documentary Trade Transactions Including Payments
1	The customer engages in transactions that are inconsistent with its business strategy (e.g., a steel company that starts dealing in paper products) or make no economic sense		X	X
2	A customer deviates significantly from its historical pattern of trade activity (i.e., in terms of markets, monetary value, frequency of transactions, volume or merchandise type)	X	X	X
3	Transacting parties appear to be affiliated, conduct business out of a residential address, or provide only a registered agent's address	X	X	X
4	Customer conducts business in jurisdictions that are at higher risk for money laundering, terrorist financing or other financial crimes	X	X	X
5	Customer shipping items to, through or from higher money laundering risk jurisdictions, including countries identified by the Financial Action Task Force as "noncooperative jurisdictions" in regard to anti-money-laundering regulations			X
6	Customers transacting in activities/goods that potentially involve a high risk of money laundering and other financial crimes, including activities/goods that may be subject to export/import restrictions		X	X
7	Obvious over- or underpricing of goods			X
8	Obvious misrepresentation of quantity of goods shipped			X
9	The payment terms or tenor are inconsistent with the type of goods			X
10	Transaction structure and/or shipment terms appear unnecessarily complex or unusual and designed to obscure the true nature of the transaction			X
11	The Letter of Credit ("LC") contains non-standard clauses or phrases or has unusual characteristics			X
12	The LC is frequently significantly amended for extensions, changes to the beneficiary and/or changes to the payment location			X
13	The transaction appears to involve use of front or shell companies for the purpose of hiding the true parties involved			X
14	The bank is approached by a previously unknown party whose identity is not clear, who seems evasive about its identity or connections, or whose references are not convincing, or payment instructions are changed at the last minute			X
15	Trade-related documentation under an LC or documentary collection appears illogical, altered, fraudulent, or certain documentation is absent that would be expected given the nature of the transaction			X
16	Transaction involves obvious dual use goods			X

The lists above are by no means exhaustive, but are largely representative of TBML cases identified so far from the categories of (i) trade finance, (ii) jurisdictions, (iii) nature of goods, and (iv) corporate structures. The recurring theme across all publications discussed in this section is that, in several cases, law enforcement agencies and banking supervisors

31 Bankers Association for Finance and Trade (BAFT), "Combating Trade Based Money Laundering: Rethinking the Approach," August 2017, http://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paper.pdf

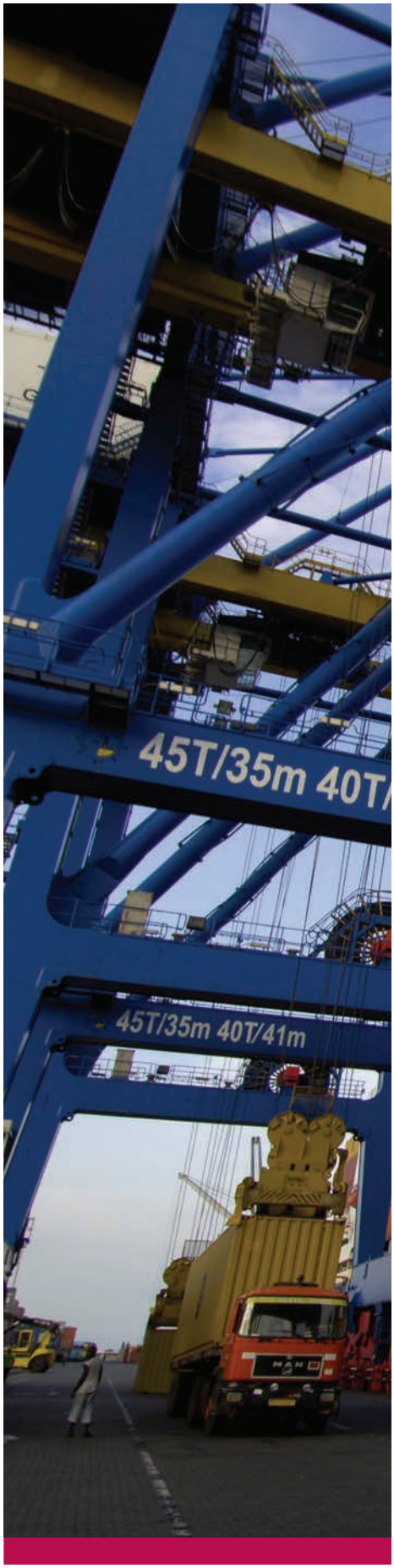
appear less capable of identifying and combating TBML than they are in dealing with other forms of money laundering and terrorist financing. This observation is probably more relevant today; as such there is a greater need for training programs on competent authorities to enhance their ability to identify TBML/FT.

Notwithstanding the limitations of regulators, banks are requested to make an effort to detect TBML/FT, as they provide services to customers that engage in trade transactions. Banks would dedicate resources and implement measures to combat TBML with the overarching principle that legitimate trading activities should not be unreasonably hindered or obstructed. These red flag lists should help banks assess the current strengths of their AML/CFT regimes in combating TBML. There may be red flags that a bank may observe in its trade finance operations but that their risk management has not identified as a TBML risk factor. Evaluating the strength of current AML/CFT regimes against these red flags may inform how existing controls, systems, and processes need to be modified to better manage TBML risks. As an example, BAFT has introduced a table of possible controls to be implemented for each transaction type:

Table 6: Recommended Controls over Trade Finance Transactions

Transaction Type	Is There an Underlying Trade Transaction?	Potential for Detecting Documentary TBML?	Do Banks See Trade Documents?	When Might a Bank See Underlying Documents?	Controls May Include:
Check Payment	Possibly	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment
Automated Clearing House (ACH) payment	Possibly	No	No	Only if specifically requested as part of a post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment
International ACH Transaction (IAT)	Possibly	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment • Potential sanctions screening (not required for domestic U.S. ACH)
Funds Transfer (Real Time Gross Settlement Payment (RTGS))	Possibly	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment • Check for completeness of payment details (depending on local regulatory requirements)
Bank-to-Bank Reimbursements	Yes	No	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds/credit check for payment
Clean Collection	Possibly	Yes	No	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Balance inquiry to ensure sufficient funds
Documentary Collection	Yes	Yes	Yes	Always	• Sanctions screening of names appearing in documents
Guarantees	Yes	Yes	Not unless specified under the terms of the guarantee	Depending on the type of guarantee	• Credit approval • Sanctions screening at issuance • Document review (including sanctions and red flags review) for payment
Standby Letter of Credit	Yes (in some cases)	Yes	Not unless specified under the terms of the standby	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Credit approval • Sanctions screening at issuance • Document review (including sanctions and red flags review) for payment
Documentary Letter of Credit	Yes	Yes	Yes	Always	• Credit approval • Sanctions screening at issuance • Document review (including sanctions and red flags review) for payment and negotiation
Supply Chain Finance	Yes	Yes	Depends on the terms of the transaction	Unless required under the terms of the financing arrangement, documents would only be seen in the event of a sanctions or monitoring trigger	• Credit approval • Sanctions screening of names • received in documentation/electronic data received • Sampling and verification of underlying transaction
Bank Payment Obligation	Yes	Yes	No, instead of documents the bank is involved in data matching	Only if specifically requested as part of a sanctions or post transaction AML monitoring trigger	• Credit approval • Sanctions screening of names received in documentation/electronic data

Real time sanctions screening of the payment should be in place for all products. Banks may also include information about whether a client uses a particular bank product in their due diligence files and also may conduct post transaction AML monitoring on account activity.



To address a number of red flag areas in TBML, the International Maritime Bureau[32] (IMB) provides authentication service for cargoes in shipment. Their survey services cover the following areas:

- Loading and discharge supervision
- Container inspection and certification
- Pre-Shipment/Pre-Insurance inspections, valuation etc.
- Quality and quantity inspection and contractual sampling in accordance with various trade associations
- Analysis of agricultural products, fertilizers, petroleum products, etc.
- Cargo space suitability
- On hire/Off hire charter surveys
- Draught surveys
- Collateral management services
- Stock auditing and monitoring
- Loss assessment and minimization, claims investigations, cargo salvage and disposal

Along with strengthening in-house capacity to detect TBML, a bank is requested to make an effort to properly investigate and, when needed, escalate to the authorities. In some high-risk jurisdictions, the banking sector may have an opportunity to assist regulators in enforcing laws against ML/FT, including TBML. Escalation is meaningful only if it results in timely enforcement action against incidences of TBML. It is advisable for a bank to discuss with its jurisdiction's financial intelligence unit (FIU) or other relevant regulatory bodies about cooperation on information sharing and how suspicious activities are to be reported. At the minimum, such a discussion should result in well-defined processes for how the FIU is to receive reports of suspicious activities, including TBML (in line with FATF recommendations 20 and 21 on reporting of suspicious transactions). Banks should expect a well-identified, clear point of contact at the FIU who is empowered to act timely with authority on reports of suspicious TBML activity.

TBML can take complex forms and continually evolves. The TBML red flag lists tabulated above are expected to grow alongside global trade flows. A bank's AML/CFT regime needs to adapt accordingly. As the first line of defense against ML/FT, ongoing training on TBML (as well as other forms of financial crime) is essential for staff of any bank. A respondent bank developing a track record of effectively combating TBML could further the trust and comfort of its correspondent banks.

32 http://www.imbship.com

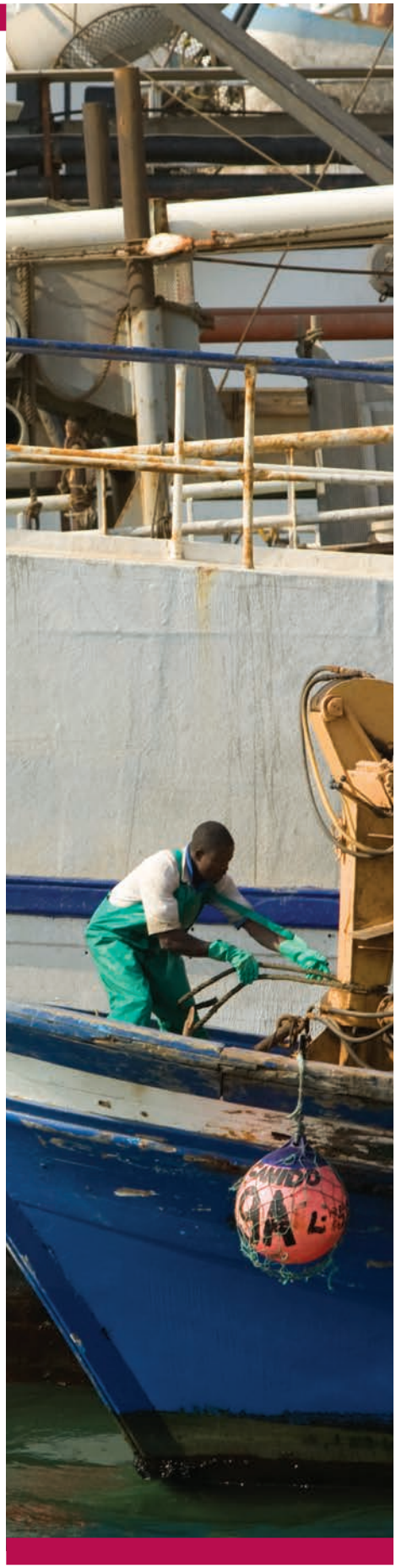
Summary of Essential Points

- Trade-based money laundering is difficult to detect since it can take complicated forms and because the scope of crimes increases alongside massive global trade flow volumes.
- In some cases, limited capacity of law enforcement agencies and banking supervisors to combat TBML is well documented. However, the duty to be proactive in combating TBML remains a core responsibility of banks. As providers of finance to legitimate trading activities, banks should dedicate resources and implement measures to combat TBML.
- This section includes red-flag indicators of trade-based money laundering.
- As the first line of defense against ML/FT, ongoing training on TBML (as well as other forms of financial crime) is essential for staff of any bank.

What This Means for Your Bank

- Be prepared for greater scrutiny from your correspondent banks over your bank's capacity to deal with TBML risks.
- Evaluate the strength of your bank's AML/CFT regime to combat TBML based on the red flag lists presented here. Implement the recommended controls as they apply to your bank.
- Train staff regularly on detection, investigation, and escalation on red flags of TBML. The red flag lists presented here are extensive but not exhaustive. They will evolve as new methodologies of TBML are discovered.
- Consult with global correspondent banks on how they are managing with TBML risks in their jurisdictions.
- Considering the limited regulatory capacity, banks should seek to exceed the minimum regulatory standards in combating TBML.
- For escalation to result in effective and timely regulatory action, establish well-defined operating procedures with FIUs on delivery of suspicious activity reports (including TBML) and exchange of other essential information.
- Collaborate with other peer banks in the market to manage TBML risks. Weak links in the banking sector in combating TBML may render your own bank's efforts to be ineffective. Sector-wide collaboration also serves to assist the regulators in augmenting their capacity in combating TBML.

V. Emerging Developments that Support AML/CFT Compliance



There are a number of emerging innovations that can contribute to both the efficiency and effectiveness of a bank's efforts at AML/CFT compliance. A few of them are highlighted below.

Legal Entity Identifiers

For a respondent bank, one basic area of due diligence to complete with a correspondent bank is establishing its identity as a legitimate entity that can open accounts. While there are a number of existing entity identifiers, Legal Entity Identifier (LEI) has become the authoritative entity identifier for regulatory reporting.[33] This was developed based on recommendations developed by the Financial Stability Board (FSB) and endorsed by the Group of Twenty (G20) international forum. This identification system assigns electronic, 20-digit, standard identifiers— LEIs—that uniquely identify legally distinct parties, thereby allowing financial connections to be identified, mapped, and linked.[34] There are about 35 accredited LEI issuers that have issued LEIs to entities in over 200 countries.[35]

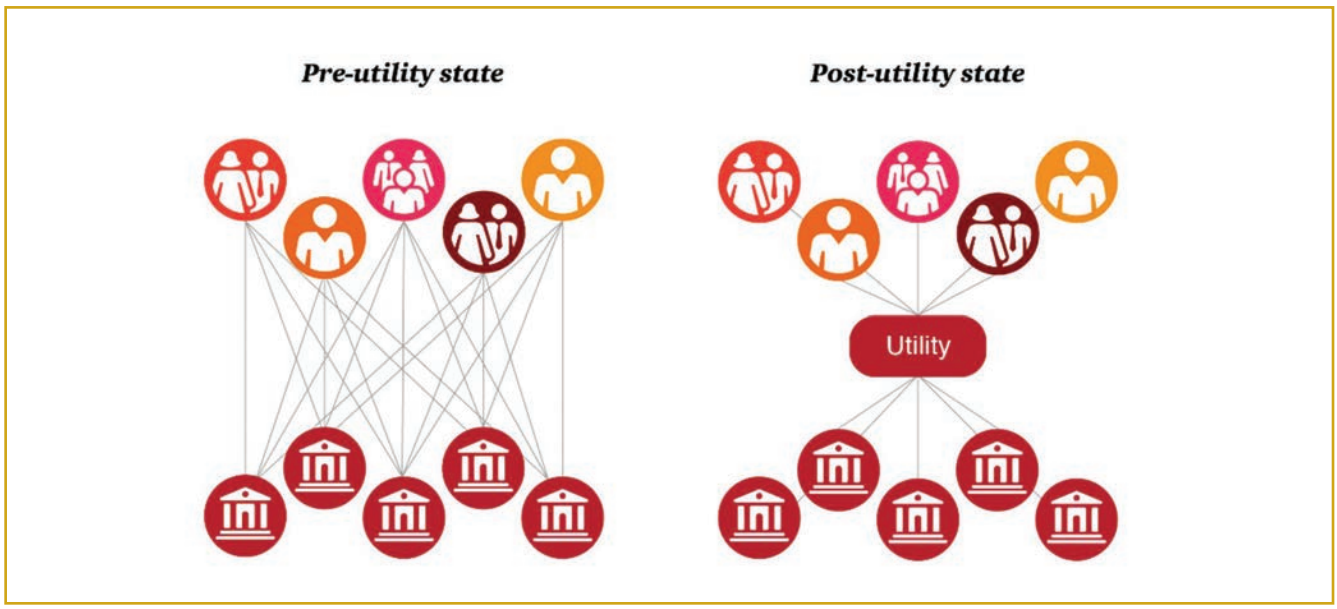
The Global LEI System is supported by the LEI Regulatory Oversight Committee (ROC) and Global Legal Entity Identifier Foundation (GLEIF).[36] They have accredited a network of organizations that are authorized to issue LEIs. As of July 2017, fees for obtaining LEI from an LEI issuer ranged from US$65 to US$119 per entity, plus there is an annual renewal requirement.[37] A respondent bank might consider adopting/obtaining LEIs in order to improve its KYC profile to correspondent bank. If a bank uses any KYC utility (described below), having an LEI may be an efficient way to establish and maintain its identity as part of its KYC disclosures to correspondent banks. Encouraging emerging market banking customers to obtain LEIs, where appropriate, would further support banks' capacity for CDD and AML/CFT.

33 SWIFT Payments Market Practice Group, "LEI in the Payments Market," September 2016, https://www.swift.com/sites/default/files/resources/pmpg_paper_leidiscussionpaper_september2016.pdf
34 McKinsey & Company, "The Legal Entity Identifier: The Value of the Unique Counterparty ID," October 2017. https://www.mckinsey.com/industries/financial-services/our-insights/the-legal-entity-identifier-the-value-of-the-unique-counterparty-id
35 Global LEI Foundation, https://www.gleif.org/en/lei-data/global-lei-index/lei-statistics
36 Ibid.
37 Ibid.

KYC Utilities

The other innovation, KYC utilities, which have several different business models, are generally third-party platforms that aim to collect banks' or corporates' information efficiently. These utilities intend to bolster a financial institution's CDD procedures by reducing redundant data submissions by respondent banks to correspondent banks.[38] KYC utilities allow a correspondent bank to use one database to monitor its respondent banks. The exhibit below illustrates how the creation of such a repository can centralize KYC activities.[39]

Exhibit 2: Pre-Utility State and Post-Utility State



There are various vendors of KYC utilities. The information requirement for a number of KYC utilities tend to mirror those reflected in the Wolfsberg questionnaire, with some variations. IFC does not endorse a specific KYC utility, but for informational purposes, a selection of vendors will be mentioned here.

SWIFT has The KYC Registry.[40] In a network of correspondent banking relationships, respondent banks can contribute KYC information on their own institution which can be consulted by correspondents upon their request and after approval by the respondent bank itself. Today, KYC Registry has more than 4,800 active banks exchanging KYC information, verified by SWIFT and in accordance to a SWIFT-defined information baseline which also includes the revised 2018 Wolfsburg Correspondent Banking Due Diligence Questionnaire (CBDDQ). Thomson Reuters also has a KYC utility solution.[41] IHS Markit is another vendor with a KYC Services platform (kyc.com).[42] IHS Markit Regulatory and Compliance offers solutions that addresses KYC requirements, regulatory requirements (EMIR, Dodd-Frank, MiFID, etc), tax validation, and 3rd party due diligence. IHS's counterparty platform has over 140,000 entities represented, including over 80,000 with LEIs. IHS recently joined forces with a blockchain firm to collaborate on blockchain solutions

38 PwC, "Share and Share Alike: Meeting Compliance Needs Together with a KYC Utility," December, 2015. https://www.pwc.com/us/en/financial-services/publications/assets/pwc-know-your-customer-utilities.pdf
39 Ibid.
40 https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/our-kyc-solutions/the-kyc-registry/features
41 https://risk.thomsonreuters.com/en/products/kyc-as-a-service.html
42 IHS Markit's KYC Services fact sheet. https://cdn.ihs.com/www/pdf/KYCServices-Sellside-factsheet.pdf

to address market needs in KYC, AML, and other key regulatory compliance areas.[43] The Bankers Almanac[44] for Risk and Compliance portfolio offers unrivalled intelligence on global financial institutions—with access to more than 23,000 banks worldwide—allowing banks to improve operational efficiency while making better-informed decisions about their correspondent banking partners. Additional modules are available, including the Bankers Almanac Due Diligence Repository, which contains over 600,000 completed KYC (such as CDD) documents, Bankers Almanac Ultimate Beneficial Ownership, which demonstrates individual beneficial ownership of entities down to 0.1%, and Bankers Almanac Regulatory Views, which identifies institutions that may require additional investigation—including state owned enterprises and sanctioned entities. With Bankers Almanac for Risk and Compliance, KYC professionals can maintain a holistic view of a counterparty using accurate intelligence that is updated regularly and verified by primary sources, to ensure quality.

In addition to being a KYC solution vendor to financial institutions, Thomson Reuters has partnered with major financial institutions to launch a national KYC service in South Africa. Participating financial institutions can access it at no charge via a web-based portal. Another form of a regional KYC solution is MANSA Platform, an initiative which is being piloted by African Export-Import Bank (Afreximbank). Afreximbank, as part of its mandate to promote intra- and extra- African trade, has taken the lead to establish a platform which is used to store customer due diligence (CDD) information, as voluntarily contributed by African financial institutions and corporate entities, while at the same time providing investment information on Africa. The objective of the Platform is to counter the effects of de-risking in Africa through reducing the cost of compliance for its African clients and improving visibility, thus, promoting good governance in Africa. The World Bank report, "The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions,"[45] mentioned two cases where regulatory authorities in Mexico and Singapore are working to develop national KYC utilities.

There are other providers of KYC utility solutions, and an emerging markets bank may be challenged to find the vendor that operates in their country and best supports its needs. National KYC utilities, such as Thomson Reuters' South Africa

43 "Cambridge Blockchain Forms Identity Data Alliance with HIS," *Business Wire*, January 31, 2018. https://www.businesswire.com/news/home/20180131005276/en/Cambridge-Blockchain-Forms-Identity-Data-Alliance-IHS

44 https://accuity.com/bankers-almanac-for-risk-and-compliance/

45 World Bank, "The Decline in Access to Correspondent Banking Services in Emerging Markets: Trends, Impacts, and Solutions: Lessons Learned from Eight Country Case Studies" 2018, http://documents.worldbank.org/curated/en/552411525105603327/pdf/125422-replacement.pdf

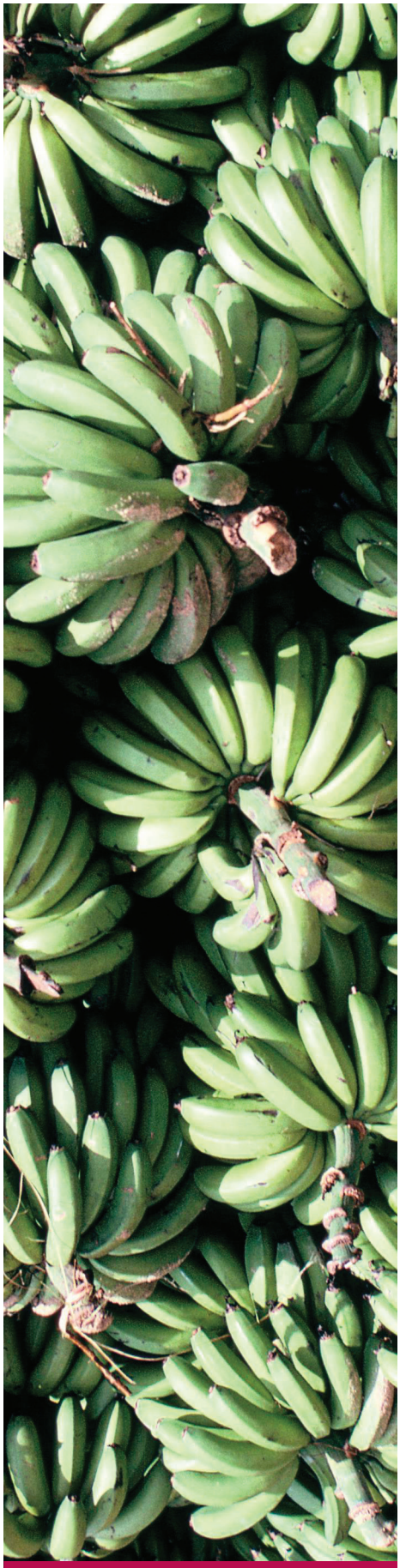
services, are not yet widely adopted. Even if a KYC utility allows a respondent bank to contribute data free of charge, the latter needs to have the appropriate internal capacity and infrastructure to submit and update all essential KYC-related information regularly and accurately. In other words, to prepare for a KYC utility, a respondent bank may need to invest in its own capacity, which (depending on the bank) could be a substantial undertaking. Examples of essential capacities needed before adopting a utility include:

- National identification systems (to establish beneficial owner of a company, for example). For banks in countries that lack such a system, LEI may be an alternative.
- For primary information that exists in non-English languages, the availability of translation services that the correspondent banks will accept.
- Other validation/certification methods to assure the correspondent banks of the authenticity of information submitted, such as data sources from primary sources (e.g. public registries).
- Systems and processes for ongoing updates and maintenance of data in the utilities in a timely manner.

This list of requirements for participation is by no means exhaustive. Many banks operate in environments where validating customer identities is difficult, or where national privacy laws limit data sharing between regulators, banks and across borders (which even limits information sharing within banks).

While such utilities may have the potential to lower due diligence and monitoring costs, they are meant to create efficiencies in the non-competitive advantage processes and they would not replace every existing procedure at a correspondent bank. The AML/CFT compliance risk is still owned by the correspondent bank. These banks remain responsible for any breach in compliance or other liability arising from the reliance of any third-party tool or method outside their own. Each correspondent bank has unique compliance requirements and risk appetite with respect to AML/CFT. Furthermore, each correspondent bank's response to ongoing evolutions in AML/CFT standards and regulations will differ over time.

As such, KYC utilities alone are not expected to materially displace institution-specific CDD processes and procedures. Conversations with correspondent banks indicate that they realize that for some aspects of due diligence, automation and delegation is not desirable. From the perspective of a respondent bank, it is uncertain whether adopting the use of a KYC utility translates into more robust correspondent banking relationships while preserving effective AML/CFT compliance. However, it is possible that working with a KYC utility would help the respondent bank more quickly understand and respond to cross-border data requests and expedite its own AML/CFT improvements. Since there is significant potential in KYC utilities for systemic



improvements, continued efforts to address the tension between facilitating more efficient data sharing and legal ML/FT accountability will contribute to efforts to prevent and/or address de-risking going forward.

For respondent banks, it may be worth having periodic dialogs with their current or potential correspondent banks regarding their use of third-party KYC utilities they use. This may help respondent banks select the most appropriate solutions and vendors for their needs. As KYC-based solutions may require relatively high upfront costs, respondent banks would need to make careful choices that best address their needs over time.

Other Initiatives

Beyond the recommendations discussed above, there is great potential to address current challenges in AML/CFT compliance with the deployment of better technologies and processes. Some notable industry-wide initiatives include the development of biometric technology; distributed ledger technology (DLT), such as blockchain; interoperability (open-sourced, real-time global payment systems) and the use of big data, driven by progress with artificial intelligence for enhanced security, among others. For example, in May 2018, a shipment of soybeans from Argentina to Malaysia was backed by a blockchain-based letter of credit; the exchange of documents for this trade was completed in 24 hours.[46]

Several of the largest global banks are independently experimenting with multiple technological innovations that may have the potential to address AML/CFT issues. IFC will continue to monitor developments in this area.

Optimized regulations that are aligned with new technologies at global, regional, and national levels could support greater standardization and harmonization for promoting global trade that is characterized by robust and efficient AML/CFT compliance.

46 Alfred Liu, "HSBC Says Trade Deal Shows Blockchain Viable for Trade Finance," *Bloomberg News*, May 14, 2018. https://www.bloomberg.com/news/articles/2018-05-14/hsbc-says-trade-deal-shows-blockchain-viable-for-trade-finance

Summary of Essential Points

- There are important emerging developments that can contribute to the efficiency and effectiveness of a bank's AML/CFT regime. They have the potential to improve a respondent bank's capacity to manage KYC processes with correspondent banks on an ongoing basis.
- There are multiple vendors of KYC utilities. There is no one-size-fits-all solution for adopting KYC utilities.
- Even if contributing data to a KYC utility is free, a respondent bank needs to have adequate internal capacity and infrastructure to submit and update all necessary data regularly and accurately. Preparing for a KYC-utility could be a substantial undertaking for a respondent bank.
- KYC utilities may have the potential to lower due diligence and monitoring costs, but they would not replace every existing procedure at a correspondent bank. The AML/CFT compliance risk is still owned by the correspondent bank.

What This Means for Your Bank

- AML/CFT related costs (including KYC) will continue to increase. Your bank will need to regularly evaluate the efficacy (both in terms of cost and effectiveness) of all elements of your AML/CFT regime to meet the necessary requirements of your correspondent banks and regulators.
- If extensive time and resources are devoted to regularly confirming your identity to your correspondent banks, consider obtaining an LEI from an accredited LEI issuer, or ask your correspondent bank if they have any other identification systems that they recommend.
- Before investing in resources to adopt a KYC utility or another solution to AML/CFT, consider asking correspondent banks what they recommend.
- New technologies for regulatory compliance (or "regtech") continues to progress. Over time, these innovations should become more cost-effective at helping your bank's KYC capacity. It would be helpful to stay current with ongoing developments in regtech as part of your resource allocation decisions behind AML/CFT compliance. As related technologies evolve, it is worth considering whether each will help you be more efficient or effective at AML/CFT.
- You might consider working with relevant institutions to join or launch KYC utility efforts.
- Any new solution should be adopted with the intent to meet international best practice in AML/CFT, not just to meet the local minimum standards.

VI. Summary of Action Items

- Be aware: correspondent banks are facing much higher scrutiny for the relationships they have with your bank and others. Respondent banks need to invest in the necessary resources to meet the global best practices of correspondent banks' AML/CFT requirements.
- Be prepared and be responsive to your correspondent bank's needs for AML/CFT and related information on your bank. Each correspondent bank may have differences in policies, information requirements, formats, reporting procedures.
- Be prepared for greater scrutiny from your correspondent banks over your bank's capacity to deal with TBML risks. Evaluate the strength of your bank's AML/CFT regime to combat TBML, based on the extensive red flag lists presented here.
- AML/CFT related costs, including KYC (more specifically, CDD) costs will continue to increase. Your bank will need to regularly evaluate the effectiveness (both in terms of cost and utility) of all elements of your AML/CFT regime to meet the necessary requirements of your correspondent banks and regulators.
- Despite competitive challenges, through objective third parties, there may be opportunities to partner with other industry participants to improve your country's ML/FT risk profile. One area where industry collaboration would be impactful is in raising the capacity of local regulators to combat ML/FT, especially with respect to TBML. Another is in the introduction of a nation-wide KYC utility, such as the one developed in South Africa. Collaboration would also help to combat more complex forms of financial crime (such as TBML), which are harder to detect.
- Be more proactive in communicating with your correspondent banks about your AML/CFT capacities. Cultivating the reputation of being a proactive and responsive respondent bank with effective AML/CFT regime will help your standing with your network of correspondent banks. Proper compliance procedures and the ability to answer questions will enhance the attractiveness of your bank in creating new correspondent banking relationships.
- There has to be a group-wide culture of zero tolerance for ML/FT. The nature of financial crime is fluid, and its detection can become more difficult. Bank staff needs to be trained on an ongoing basis.
- Banks should move towards global best practices for AML/CFT as this is what your correspondent banks will need to comply with. Your bank should integrate Wolfsberg's 2018 CBDDQ as the foundation for your institution's readiness in managing correspondent banking relationships. The CBDDQ is already integrated in some KYC utilities developed by third-party vendors.
- It is important to thoroughly know your customers at all times: who they are (robust identity verification), what their normal banking activities are, where did their assets originated from, etc. Beneficial ownership needs to be unpacked to identify the ultimate beneficial owners.
- Your bank's AML/CFT regime requires systems, processes, and procedures that are cost-effective in managing ML/FT risks to meet international best practices in AML/CFT, not just to meet the local minimum standards.


QC 02
NYK
45
tex

Glossary

Beneficial Owner

The natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

De-Risking

The actions by financial institutions terminating or restricting their relationships with customers or categories of customers in order to avoid risk.

Enhanced Due Diligence

Additional due diligence measures applied by a correspondent bank beyond their standard customer due diligence on counterparties based in countries deemed to be high risk.

Financial Action Task Force

An inter-governmental body established in 1989, with the objectives to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

Financial Crime

Includes but is not limited to money laundering, fraud, tax evasion, human trafficking, bribery and corruption, terrorist financing, the financing of proliferation of weapons of mass destruction and other related threats to the integrity of the international financial system.

Financial Intelligence Unit (FIU)

A government entity that serves as a national center for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis.

Financing of Terrorism

The financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism.

KYC Utilities

A KYC utility is a central repository that stores the data and documents required to support a financial institution's CDD procedures.

Money Laundering

A financial crime in which proceeds from a criminal activity are disguised through the financial system to conceal their illicit origins.

Nested Relationships

The use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services.

Payable-Through Accounts

Correspondent accounts that are used directly by third parties to transact business on their own behalf.

Risk-Based Approach

Within the framework of FATF's requirements, the adoption of a flexible set of measures to implement the FATF recommendation that targets resources effectively and commensurate with the nature of ML/FT risks faced by a bank.

Shell Bank

A bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Trade-Based Money Laundering

The process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins.

Wolfsberg Group

An association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to know your customer, anti-money laundering and counter terrorist financing policies.

Appendix A: FAFT's 40 Recommendations

THE FATF RECOMMENDATIONS		
Number	Old Number	
		A – AML/CFT POLICIES AND COORDINATION
1	–	Assessing risks & applying a risk-based approach
2	R.31	National cooperation and coordination
		B – MONEY LAUNDERING AND CONFISCATION
3	R.1 & R.2	Money laundering offence
4	R.3	Confiscation and provisional measures
		C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION
5	SRII	Terrorist financing offence
6	SRIII	Targeted financial sanctions related to terrorism & terrorist financing
7		Targeted financial sanctions related to proliferation
8	SRVIII	Non-profit organisations
		D – PREVENTIVE MEASURES
9	R.4	Financial institution secrecy laws
		Customer due diligence and record keeping
10	R.5	Customer due diligence
11	R.10	Record keeping
		Additional measures for specific customers and activities
16	SRVII	Wire transfers
12	R.6	Politically exposed persons
13	R.7	Correspondent banking
14	SRVI	Money or value transfer services
15	R.8	New technologies
		Reliance, Controls and Financial Groups
17	R.9	Reliance on third parties
18	R.15 & R.22	Internal controls and foreign branches and subsidiaries
19	R.21	Higher-risk countries
		Reporting of suspicious transactions
20	R.13 & SRIV	Reporting of suspicious transactions
21	R.14	Tipping-off and confidentiality
		Designated non-financial Businesses and Professions (DNFBPs)
22	R.12	DNFBPs: Customer due diligence
23	R.16	RDNFBPs: Other measures

		E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24	R.33	Transparency and beneficial ownership of legal persons
25	R.34	Transparency and beneficial ownership of legal arrangements
		F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
		Regulation and Supervision
26	R.23	Regulation and supervision of financial institutions
27	R.29	Powers of supervisors
28	R.24	Regulation and supervision of DNFBPs
		Operational and Law Enforcement
29	R.26	Financial intelligence units
30	R.27	Responsibilities of law enforcement and investigative authorities
31	R.28	Powers of law enforcement and investigative authorities
32	SRIX	Cash couriers
		General Requirements
33	R.32	Statistics
34	R.25	Guidance and feedback
		Sanctions
35	R.17	Sanctions
		G – INTERNATIONAL COOPERATION
36	R.35 & SRI	International instruments
37	R.36 & SRV	Mutual legal assistance
38	R.38	Mutual legal assistance: freezing and confiscation
39	R.39	Extradition
40	R.40	Other forms of international cooperation

Appendix B: List of Relevant Key Documents for this Publication

Resources from FATF

International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation – The FATF Recommendations. February 2018.
http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF Guidance on Correspondent Banking Services. October 2016.
http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Correspondent-Banking-Services.pdf

FATF Guidance on AML/CFT Measures and Financial Inclusion, with a Supplement on Customer Due Diligence. November 2017.
http://www.fatf-gafi.org/fr/publications/inclusionfinanciere/documents/financial-inclusion-cdd-2017.html?hf=10&b=0&s=desc(fatf_releasedate)

Trade Based Money Laundering. June 2006.
http://www.fatf-gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf

Best Practices on Trade Based Money Laundering, June 2008.
http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

APG Typology Report on Trade Based Money Laundering.
http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

Resources from the Wolfsberg Group

SWIFT Relationship Management Application (RMA) Due Diligence. 2016.
https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/7.%20SWIFT-RMA-Due-Diligence.pdf

Payment Transparency Standards.2017.
https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf

Trade Finance Principles jointly drafted with ICC and BAFT. 2017.
https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/comment-letters/6.%20Trade-Finance-Principles-Wolfsberg-Group-ICC-and-the-BAFT-2017.pdf

Anti-Money Laundering Principles for Correspondent Banking. 2014.
https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/8.%20Wolfsberg-Correspondent-Banking-Principles-2014.pdf

Correspondent Banking Due Diligence Questionnaire .2018.
https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/Wolfsberg%27s_CBDDQ_220218_v1.2.pdf

Other Sources

International Chamber of Commerce: Rethinking Trade & Finance. 2017.
https://iccwbo.org/publication/2017-rethinking-trade-finance/

Basel Committee on Banking Supervision: Guidelines – Sound Management of Risks Related to Money Laundering and Financing of Terrorism. June 2017. https://www.bis.org/bcbs/publ/d405.pdf

International Finance Corporation: De-Risking and Other Challenges in the Emerging Market Financial Sector. Findings from IFC's Survey on Correspondent Banking. September 2017. http://documents.worldbank.org/curated/en/895821510730571841/pdf/121275-WP-IFC-2017-Survey-on-Correspondent-Banking-in-EMs-PUBLIC.pdf

Society for Worldwide Interbank Financial Telecommunication (SWIFT). Payments Market Practice Group: LEI in the Payments Market. November 2017. https://www.swift.com/about-us/community/swift-advisory-groups/payments-market-practice-group/document-centre/document-centre

PwC: Share and Share Alike: Meeting Compliance Needs Together with a KYC Utility. December 2015.
https://www.pwc.com/us/en/financial-services/publications/assets/pwc-know-your-customer-utilities.pdf

McKinsey & Company: The Legal Entity Identifier: The Value of the Unique Counterparty ID. October 2017.
https://www.mckinsey.com/industries/financial-services/our-insights/the-legal-entity-identifier-the-value-of-the-unique-counterparty-id

Bankers Association on Finance and Trade (BAFT): Combating Trade Based Money Laundering: Rethinking the Approach. August 2017. http://baft.org/docs/default-source/marketing-documents/baft17_tmbl_paper.pdf

For further information on our trade and supply chain products, please contact our team.

MANAGEMENT TEAM

Hyung Ahn
Global Head, Trade and Commodities
T: +1 202 458 9288
E: HAhn@ifc.org

Inho Lee
Head, New Products
T: +1 202 458 2709
E: ILee@ifc.org

Makiko Toyoda
Acting Head of GTFP
T: +1 202 473 7196
E: MToyoda@ifc.org

BUSINESS DEVELOPMENT & GTFP

Global Banks

Zeynep Ersel
Business Development Lead
T: +1 202 458 2502
E: ZErsel@ifc.org

Asia & the Pacific

Anurag Mishra
Regional Lead
T: +91 77 3870 7535
E: AMishra4@ifc.org

Gimhani Seneviratne
Sr. Trade Finance Officer
T: +66 2 686 6532
E: GTalwatte@ifc.org

Lien Hoai Nguyen
Trade Finance Officer
T: +84 4 3934 2282 x603
E: NLienHoai@ifc.org

Alok Kumar
Trade Finance Analyst
T: +91 22 4230 2400
E: AKumar25@ifc.org

Europe & Central Asia

Aleksey Nikiforovich
Regional Co-Lead
T: +7 495 411 7555 x2129
E: ANikiforovich@ifc.org

Mark Rozanski,
Regional Co-Lead
T: +1 202 473 4640
E: MRozanski@ifc.org

Latin America & the Caribbean

Susanne Kavelaar
Regional Lead
T: +54 11 4114 7229
E: SKavelaar@ifc.org

Raquel Segrera
Trade Finance Officer
T: +57 1 319 2374
E: RSegrera@ifc.org

Giorgio Felici
Associate Trade Finance Officer
T: +54 11 411 47 213
E-mail: GFelici@ifc.org

Karla Lopez
Trade Finance Analyst
T: +1 202 458 8683
E: KLopezflores@ifc.org

Middle East & North Africa

Ahmed Hanaa Eldin Mohamed,
Regional Lead
T: +20 2 2461 4275
E: AMohamed5@ifc.org

Zeynep Attar
Associate Trade Finance Officer
T: +90 212 385 1329
E: ZAttar@ifc.org

Sub-Saharan Africa

Florian Wicht
Regional Lead
T: +27 11 731 3025
E: fwicht@ifc.org

Alexei Timofti
Southern and Eastern Africa Lead
T: +27 11 731 3171
E: ATimofti@ifc.org

Benie Kouakou
West Africa Lead
T: +22 52 240 0438
E: BKouakou@ifc.org

TRADE OPERATIONS

Murat Ayik
Head of GTFP Operations
T: +90 212 385 2579
E: MAyik@ifc.org

Hande Berdan
Associate Trade Finance Officer
T: +90 212 385 2523
E: HBerdan@ifc.org

Sinan Onat
Trade Finance Analyst
T: +90 212 385 2594
E: SOnat@ifc.org

Fide Maksut
Trade Finance Analyst
T: +90 212 385 3094
E: FMaksut@ifc.org

Gizem Ayaz
Trade Finance Analyst
T: +90 212 3852567
E: gartuk@ifc.org

Ozge Etcan
Trade Finance Analyst
T: +90 212 385 2575
E: oetcan@ifc.org

Yasser Hassan
Trade Finance Analyst
T: +1 202 458 0183
E: YHassan@ifc.org

Dharmendra Deepak
Operations Officer
T: +1 202 473 8817
E: ddeepak@ifc.org

Ebrahim Farouk
Portfolio Officer
T: +1 202 473 0863
E: EFarouk@ifc.org

Fiona Chen
Associate Operations Officer
T: +1 202 458 2545
E: FChen1@ifc.org

Virginia Ziulu
Associate Operations Officer
T: +1 202 473 4410
E: VZiulu@ifc.org

Jessica Kim
Associate Operations Officer
T: +1 202 473 6362
E: JKim21@ifc.org

Beatrix Von Heintschel
Trade Finance Analyst
T: +1 202 473 0071
E: bvonheintschel@ifc.org

Corrine Harrison
Operations Assistant
T: +1 202 473 8812
E: Charrison@ifc.org

Mauricio Cifuentes
Operations Assistant
T: +1 202 473 4516
E: MCifuentes@ifc.org

Structured Trade Commodity Finance/ Global Warehouse Finance Program (GWFP)

Pierre Ligneul De Villeneuve
Sr. Investment Officer
T: +1 202 473 94 23
E: PLigneul@ifc.org

Gregory Lorne
Investment Officer
T: +1 202 458 5424
E: GLorne@ifc.org

Lili Wang
Financial Officer
T: +1 202 458 9626
E: LWang14@ifc.org

Portfolio Solutions (GTLP & CCFP)/ Working Capital Systemic Solutions (WCSS)

Juan Andres Mosquera
Sr. Investment Officer
T: +1 202 458 5152
E: JMosquera@ifc.org

Heather Miller
Operations Officer
T: +1 202 458 5218
E: HMiller1@ifc.org

Global Trade Supplier Finance (GTSF)

Nevin Turk
Product Lead
T: +1 202 458 4786
E: NTurk@ifc.org

Global Strategy

Susan K. Starnes
Senior Strategy Officer
T: +1 202 473 6439
E: SStarnes@ifc.org

Arun Prakash
Strategy Officer
T: +1 202 473 6095
E: APrakash@ifc.org

Administrative Support

Inosha Wickramasekera
Program Assistant
T: +1 202 458 0991
E: IWickramasekera@ifc.org

Jasmine Meesarapu
Program Assistant
T: +1 202 458-2674
E: jmeesarapu@ifc.org

2121 Pennsylvania Ave. NW
Washington, DC 20433
Tel. 1-202-473-1000
www.ifc.org/sustainability
asksustainability@ifc.org