FRESH IDEAS ABOUT BUSINESS IN EMERGING MARKETS EMCompass

www.ifc.org/thoughtleadership NOTE 59 • OCT 2018

How a Know-Your-Customer Utility Could Increase Access to Financial Services in Emerging Markets

Global efforts to counter terrorism financing and money laundering have led banks to terminate relationships with some communities, businesses, and individuals around the world. When a financial institution or intermediary cannot easily judge the identity and associated risks of a customer, it is often more efficient to avoid transacting with that customer altogether. This may disproportionately affect small banks, small firms, and low-income individuals in emerging and developing economies. This Compass Note explores an innovative solution that could help improve customer due diligence through a Know-Your-Customer (KYC) utility.

Knowledge of a customer is central to providing financial services, so effective and efficient customer due diligence (CDD) is critical to enabling financial intermediaries to serve their customers. Over the last 20 years, financial intermediaries have also been expected to monitor for, and report on, potential financial crimes. Failure to do so can result in large fines or termination of operations.

The increasing complexity of this law enforcement role, and associated reporting and monitoring requirements and costs, have caused some financial intermediaries (FIs) to pull back from cross-border investment, trade, and clearing and settlement activities. When correspondent banks withdraw from relationships with respondent banks and other FIs, this is collectively referred to as de-risking. This usually implies that the correspondent was unable to cost effectively assess the quality of a counterparty's CDD processes, and therefore cannot assess the risks. As a result, the FI often terminates the relationship with that counterparty. This has had systemic impacts in some smaller countries, and particularly in those countries without a global correspondent bank willing to clear and settle U.S. dollar transactions.

Know-Your-Customer (KYC) utilities may be a solution. This note explores how International Financial Institutions (IFIs), Multilateral Banks (MDBs), private firms, and governments could work together to develop KYC utilities. These could help improve CDD in smaller or more difficult emerging markets and have the ultimate goal of improving integration and financial inclusion.

What is KYC?

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing, and the proliferation of weapons of mass destruction. FATF has developed the following basic principles for customer due diligence that are required to "Know a Customer."

Who is the customer? – Establish Identity. For individuals, identify the customer and verify his or her identity using reliable, independent source documents, data, or information. For companies, identify the name, legal form, existence, and beneficial owner(s), and verify their identities.

What are customers doing? – Transaction Monitoring and Ongoing Customer Due Diligence. Understand the purpose and intended nature of relationships between individuals and businesses. Where is the money coming from into the institution and how is it being used?

Conduct ongoing customer due diligence to ensure that customer transactions match customer profiles. Ongoing CDD involves tracking mergers and acquisitions; reviewing new lines of business; investigating changes in governance, directors, and management; and being sure that customer profiles are up-to-date.

In many countries, if these transaction monitoring processes or ongoing customer due diligence processes reveal any suspicious transactions or activities, then the FI is legally obligated to report this to the national law enforcement authorities for further investigation. Failure to report can result in fines and/or loss of the FI's operating license.

CDD Risks and De-risking

For individuals or firms to receive formal financial services, they must have a verifiable identity and valid transaction records. Transactions must conform to customer profiles, and when they do not, the customer must explain the transaction or it will be rejected. For any suspicious transaction, a report must be filed with the authorities.

Correspondent banks must be able to verify that respondent banks are doing sound CDD and are reporting possible crimes to avoid the inadvertent processing of criminal transactions. In many cases, if a correspondent bank cannot easily and affordably assess the legitimacy and risks of a respondent bank's transactions, it will simply terminate the relationship. Unfortunately, small banks, small money transfer organizations, charitable organizations, small firms, and poor people are often disproportionately affected by CDD requirements. Their transactions are often cash-based or cannot be traced, and the returns from transacting with them are small, making the risks of dealing with these entities larger than the rewards. Similarly, respondent banks will feel pressure to terminate relationships with low-income individuals and small firms if validating transactions with them is prohibitively expensive. The consequences of this have been reductions in trade, remittances, and credit availability, as well as diminished financial performance and job losses.

Thus, an unintended consequence of Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulations has been that global correspondent banks have withdrawn operations in smaller markets and no longer collaborate with local banks that serve smaller customers. The knock-on effect of this de-risking is reduced services to some of the poorest and most stressed countries exactly when their integration into global trade and supply chains and the global financial system is critical to their recovery. Know-Your-Customer utilities could help resolve this problem.

What is a Know-Your-Customer Utility?

There are three types of KYC utilities operating today: **Industry Collaboration Utilities, Jurisdictional Utilities,** and **Utility Service Providers**. Two subcategories of utility service providers are: a) **Utility Services**, which are primarily data services and identification (ID) information storage; and b) **Managed Services**, which are basically outsourced utility services, plus transaction tracking and CDD. Examples of each type of utility are as follows:

Industry Collaboration Utility: SWIFT

CDD requires records of where customer payments originate and terminate. This explains why one of the first successful KYC utilities was introduced by SWIFT, the Society for Worldwide Interbank Financial Telecommunications.

Essentially, SWIFT deals in electronic messages between banks, and these messages provide a transaction trail, documenting where money originates and terminates. SWIFT does not clear or settle transactions, and holds no accounts, but does pass information about payments through its highly secure messaging system. SWIFT has a successful shared data repository that holds profile data for hundreds of respondent and correspondent banks. The SWIFT KYC utility, available to SWIFT members, is useful for member correspondent/respondent banking relationships, and reduces correspondents' risk when dealing with respondent banks in high-risk or sanctioned jurisdictions because the SWIFT utility validates where the money goes, and that the recipient is acceptable. The utility, which is used by major correspondent and respondent banks, is used primarily for the larger payments of larger corporations. There are around 11,000 SWIFT users today, which makes SWIFT a significant player in international corporate payments; however, many smaller banks and FIs in emerging markets are not SWIFT members.

Jurisdictional Utility: Monetary Authority of Singapore KYC Utility

The Monetary Authority of Singapore has introduced a National KYC utility that covers all individuals with accounts in Singapore. The "MyInfo" service, a personal data platform that contains government verified personal details for every account holder, is the foundation for this utility. Residents provide their data to the government once,

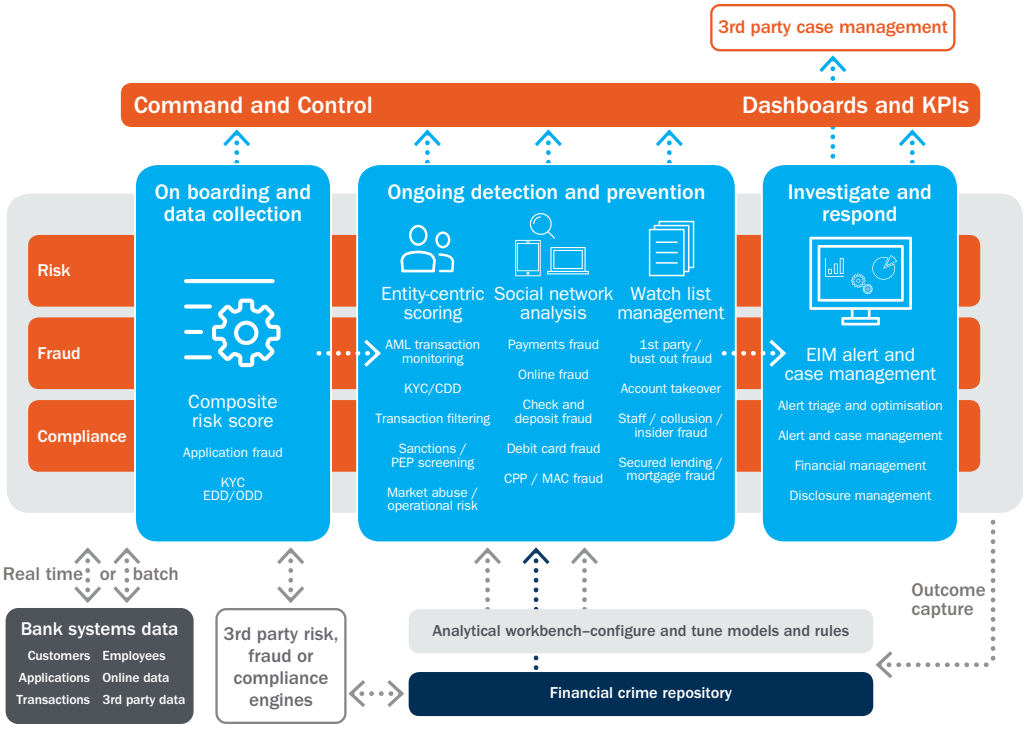

FIGURE 1 BAE's KYC Utility Product Offering—The NetReveal risk, fraud, and compliance solution suite.

Source: www.baesystems.com

and it then supports all subsequent online transactions. The goal is to link all FIs to this validated database, which will reduce redundancy and improve information quality. Singapore has the advantage of a very good national ID system and database, and the nation is highly digitally enabled. Its utility does not address transaction monitoring or ongoing CDD; that role is retained by the individual FIs.

Utility Service Provider: BAE Systems

BAE Systems is the largest defense contractor in the world, and offers its "NetReveal" product as a managed service for CDD/KYC solutions. This enterprise-wide approach is intended to satisfy all CDD/KYC requirements for the financial institutions (primarily European banks) that outsource financial functions to BAE. BAE's system includes customer information capture, validation, risk rating, politically exposed person (PEP) checking, investigation, regulatory reporting, continuous monitoring, beneficial ownership validation, risk ratings, changes in management, adverse events, business expansion, new lines of business, initial public offerings (IPOs), acquisitions, divestitures, geographic expansion, social media coverage, credit rating changes, etc. The system also monitors transactions and uses artificial intelligence (AI) and other applications to automate most of these activities (**Figure 1**).

Potential Impacts of a KYC Utility

Widespread use of KYC utilities could deliver three major gains:

1) Better CDD information could lead to less corruption, tax evasion, money laundering, and other criminal activities.

2) KYC utilities could process information more consistently, in more consistent formats and requests, and at lower cost, which would leverage economies of scale for data, among other attributes. This could make financial services more accessible and more profitable at lower transaction sizes, and lower volumes, and thereby increase financial inclusion and the expansion of financial networks. This could make correspondent banking relatively less expensive for both correspondent and respondent banks.

3) KYC utilities can provide better information management, with higher reliability, because information is more comprehensive across all institutions and is cross-validated, which improves accuracy. This reduces the risks of doing business with customers, and thereby can reduce the pressure on banks to sever relationships, while also making it cheaper and easier to create new relationships because the cost of CDD is lower, and information is more reliable.

When KYC utilities are coupled with digital financial services

(DFS) and other IT applications, gains can be amplified. Information technology can be used to process and track transactions in ways that further reduce risks and processing costs, to the point that universal financial access becomes economically feasible on a commercial basis. In markets with extensive mobile phone penetration, the marginal cost of processing digital payments is approaching zero.

Ironically, it is not processing costs but KYC/AML risks and CDD compliance costs that are creating barriers to integration and inclusion. Artificial intelligence and machine learning offer ways to improve data analysis and identify problematic transactions cheaply and quickly. New blockchain applications such as the R3 Corda Platform, are also offering improved KYC data management and reliability. If DFS continues to reduce the use of cash, transaction monitoring costs will plummet, while transparency increases, further reducing criminal activity and supporting universal financial inclusion.

A KYC utility would **not** assume a financial intermediary's KYC risks, nor would it assume any liability associated with AML/CFT risks. It would only assure FIs that their customers have been more fully and effectively vetted and tracked, using a larger number of data sources, processed by better informed AI engines, and delivered at lower cost. If a customer was subsequently caught laundering money through a bank that uses the utility, that bank would still be responsible, and would still bear the regulatory and financial risks associated with this breach.

Positive KYC utility impacts are possible. U.S. money center banks generally agree that KYC utilities would improve CDD reliability and reduce risks in a cost-effective manner. There is also agreement that using these utilities would reduce the risks of providing correspondent banking services to respondent banks.

KYC utilities could also reduce risks and improve returns. A KYC utility could shift the risk/return threshold in a way that increases financial inclusion and access in many countries. This would have the greatest impact on smaller customers, and smaller transactions in smaller countries. This could be done by increasing the quality and speed of verifying customer identities; improving the speed and effectiveness of transaction monitoring; improving the speed and effectiveness of customer monitoring and ongoing CDD; improving data integrity through more comprehensive and complete information across systems; and performing transactions at lower cost.

Also, risks could be reduced and returns improved by coupling a KYC utility with improved automation, tiered risk-based processes (see below), and the application of basic decision rules, algorithms, and cross-validation techniques. KYC utilities could effectively deploy these additional tools at scale.

KYC utilities can be more effective, reliable, and cheaper than spreading KYC activities across multiple players, but there are four additional requirements that KYC utilities should meet:

1. **They need to reach a certain scale to be profitable.** Scale can be achieved by working with a single, very large bank or by working with many smaller banks.
2. **They need multiple layers of data and privacy protection**; therefore, cybersecurity and data redundancy are also central to a utility's ability to operate successfully.
3. **AI and machine learning** are required core technology for successful KYC utility operations due to their ability to reduce costs and improve accuracy.
4. **They require regulatory backing to be successful.**

What is Required to Support Effective KYC Utilities?

For a country to establish or participate in a KYC utility, there are six basic prerequisites:

1. **Individuals and companies must have unique, verifiable identities.** Identity varies by country, and could be based on government services, or could be provided by the private sector. For individuals, identity could be based on records such as a national or state ID, driver's license, passport, or biometric identity system such as Aadhaar in India, which uses retina scans and fingerprints to establish unique biometric IDs. The "Big 4" banks in South Africa created a private biometric system that covers about 80% of the financial services market. This allows the banks to use on-line finger print verification, linked to the National Identification System.

   For companies, a unique company identifier linked to legal form and beneficial owners is also required. A KYC utility could bring all identity records together in one place and make these easier to access, validate, and cross-reference, ensuring better monitoring.
2. **Transactions must be monitorable.** FIs are responsible for monitoring and reporting any suspicious transactions, and must have procedures to ensure this. The current processes, which are fragmented across

banks, are expensive and create higher systemic risk. This is because each FI only knows data from its own processes and does not have access to all the knowledge within the financial system. As a result, there is excess cost and unexploited information in the system that individual institutions cannot access. Other than people or firms placed on a "black list" by authorities, typically, little information is shared among FIs; and in some jurisdictions, such information sharing is illegal.

A KYC utility could help to solve these problems by enabling access to all customer information in one place, for viewing by people authorized to assess CDD risks. In addition, transaction monitoring increasingly uses big data and artificial intelligence to discover suspicious transactions across the entire system. A KYC utility is well positioned to do this. In many countries, implementation would require regulatory changes regarding data sharing. These could include a form of identity "blinding" or a standard set of permissions, to which all customers participating in the utility must agree.

3. **Customers must be monitorable.** In addition to transaction records, other customer data must be linked to IDs. This includes meaningful information about individuals or firms, and their sources and uses of funds. Banks often struggle to get consolidated customer information, or information on related parties, and many lack detailed customer information or electronic records about where a customer gets money. Or banks have no knowledge about how a customer spends money. Banks often struggle to maintain active, up-to-date customer files. Some banks do this well, but many do not. This is because many banks have legacy IT systems built around product applications (deposits, loans, etc.), and not around customers, and for some banks, compliance management is still manual. Many smaller banks in smaller countries have this problem, hampering their CDD effectiveness.

   KYC utilities could help by centralizing customer information files around a unique customer ID, and making this information available on a permissioned basis. Customers could decide with whom they would share information, but all information would be available in one place, and would be easy to monitor for suspicious transactions. In effect, this would result in smaller banks outsourcing their customer file management to the KYC utility, which could greatly help these smaller banks.

4. **Smaller accounts might be ignored.** Another option would be to ignore smaller transactions and accounts. Low-income individuals typically do not have much money and do not engage in large financial transactions, yet CDD requirements are often the same for rich or poor. Governments can take a risk-based approach to determine which customer transactions are worth examining. Mexico has implemented a tiered CDD system based on the size of a customer's balances, and the size and frequency of transactions. Below a certain level, customers do not require formal IDs. As the size of balances and transactions increases, ID requirements also increase. In Mexico, this tiered ID system has eliminated the need to scrutinize some 80% of FI accounts. Only customers whose balances exceed $3,700 are required to present formal IDs. KYC utilities could take advantage of this kind of tiered risk-based system to reduce costs and could improve customer tracking as they move up tiers.

5. **Maintaining data privacy and cybersecurity is critical.** A KYC utility could be subject to abuse. Private information wrongly revealed about individuals could expose them to expropriation risks. Information could also be used to discriminate against individuals based on their race, gender, or other characteristics. Inaccurate information could be entered into a system with the intention of defrauding or harming individuals or firms. Centralizing information makes it more vulnerable to abuse, and increases the need for cyber-security and other controls that prevent abusive practices. Thus, any country that approves a KYC utility needs to address these risks and create appropriate controls and back-up systems to ensure security and stability. The Aadhaar experience in India offers a good case study on these issues.

6. **Good governance and correct incentives are essential.** KYC utilities manage and maintain large amounts of confidential information that is subject to a wide variety of potential abuses. For these reasons, they require careful management and governance. A country that establishes such a utility needs to carefully consider appropriate governance and incentives to maintain high data integrity, security, and reliability. These issues are discussed in greater detail below.

Why Should Governments Support a KYC Utility?

Governments concerned about money laundering, corruption, tax evasion, terrorist financing, and other

illegal activities, as well as data privacy and cyber security, should embrace KYC utilities to help address these issues. Not all governments want transparency and integration, and in these cases, KYC utilities are unlikely to be helpful, and could be harmful or subject to abuse. But for governments that are committed to being part of the global financial system, KYC utilities could help with information management, and leverage other government policies that move a country away from cash, and to using digital financial services. In most cases, KYC utilities can mutually reinforce changes that help countries reduce certain types of crime, improve productivity, increase financial inclusion; and potentially improve trust in AML/CFT capacity, and increase integration and economic growth.

Why Would Large International Correspondent Banks Support Local KYC Utilities?

In discussions with IFC, several leading international banks have expressed support for developing local KYC utilities. This is based on the belief that such utilities could have more complete information, and would be able to validate this information more quickly, more reliably, and less expensively than the current institution-by-institution approach in local markets. To a large extent, global correspondent banks face both individual institutional risk and local regulatory risk in dealing with local banks in each country. In the same way that a local bank's credit rating is capped by its government's sovereign risk rating, local KYC regulations and enforcement are weighted heavily in the assessment of the KYC risk for an individual financial institution within that jurisdiction. A bank's KYC risk is often delimited by the effectiveness of local KYC regulations and enforcement. To the extent that local KYC utilities could improve information quality and reliability, they could help global correspondent banks to justify delivering services to markets that are currently excluded.

Why Would Local FIs Support KYC Utilities?

Local FIs would benefit from more efficient information collection and management, and over time, would also benefit from a more comprehensive database. However, dominant players in local markets could view the utility's services as using their proprietary data to benefit their competitors. This, in turn, raises issues about incumbency advantage, fair competition, and data ownership, which must be resolved in each market.

Why Would Local Private Enterprises Support KYC Utilities?

Given the potential economic benefits of an integrated market—including more imports, exports, foreign investment, financing flows, and knowledge sharing—the local private sector should support KYC utilities and information transparency. As long as these utilities make interactions with the global community less expensive, and more secure, consistent, available, and reliable, there should be broad-based support for them. However, information sharing requirements may increase in some jurisdictions, which will increase time spent and complexity for private sector banking customers. A KYC utility can help monitor and manage these issues.

KYC Utility Ownership Considerations

Because a KYC utility accesses and holds highly confidential data, strong management and governance are needed to prevent abuse by either government or the private sector. This is true even if the KYC utility is predominately a jurisdictional "identity database", and even more important if the utility takes on additional roles.

Thus, strong checks and balances are needed to protect the integrity of KYC utilities. Depending on the specific country, the utility might be a public-private partnership (PPP) or a government regulated and supervised private sector entity such as a private credit bureau or a government-owned and regulated utility, or some hybrid of these. The challenge will be to balance transparency and privacy concerns, as well as efficiency and scope of coverage. Careful attention must be paid to governance, individual rights, operating efficiency, and the structure of the incentives for the utility. Experiences with credit bureaus make it clear that poorly run and poorly governed utilities can destroy value. It is also clear that public listing can help align incentives so that shareholders more actively govern a utility's management. As we have seen with the Equifax data breech in 2017, share price declines proved to be a strong corrective force.

KYC Utility Ownership Structures and Management

Beyond being a publicly listed company, other possible KYC utility ownership structures include joint ownership by all local FIs, or full or partial government ownership. In the initial stages, IFC or other international financial institutions or donors could be minority investors, and their influence could help with the utility's establishment and governance. Operational management could be

in-house or outsourced, depending on the situation and the availability of qualified firms and people. The utility might start-out as a PPP, with a professional service firm operating under a "build-operate-transfer" structure that could eventually place the utility under local private sector management, and the utility's shares under public ownership, governed by an independent board, and supervised by an independent government entity. However, for this to work, the utility would need to be profitable. This implies that it would need to operate at sufficient scale to make money, which would require it to be a regional or global, rather than a national, entity.

However, regional or global utilities often face insurmountable challenges in harmonizing national laws and regulations, and are therefore difficult to establish. In addition, cross-border co-ownership structures are often fragile, and the withdrawal of one or two participants could damage them irreparably. Such a utility would need to offer sufficient value to justify the revenue it expects to collect, and the full realization of that value may not be entirely within its control (subject to jurisdictional, financial information, and information architecture limitations). For these reasons, publicly listed national utilities are more likely to be successful. In countries where this is not possible, local governments will need to look for ways to make local or regional utilities workable—including harmonizing laws and regulations, and possibly making participation mandatory.

When KYC Utilities are Not Attractive to Private Sector Owners

In smaller markets, private ownership may not be an option, making government ownership the only choice. In these cases, governments would need to realize enough benefits from the KYC utility to justify the costs of setting-up and paying to run it (with the utility's management likely outsourced to a qualified vendor). Under these circumstances, the utility would still require close regulation and supervision and, for this reason, might need to be administratively separate from the central bank and/or banking supervisors to ensure checks and balances between the regulators and the regulated.

Data Sharing Issues

Typical issues that must be addressed in initial KYC utility discussions concern who has which data, and who loses competitive advantage by sharing it. In highly concentrated financial systems, where a few banks have most of the market, it is often difficult to get these banks to share their data, even if they are offered ownership shares in the utility. Customer data is considered proprietary and a source of competitive advantage, and FIs believe that they "own" this data, and will often refuse to share it, particularly if other FIs might benefit. This incumbency advantage is a problem in many countries, and can be even more difficult if the largest FIs are also state owned. In these cases, governments can mandate participation in a utility, but difficult negotiations may be needed to get larger FIs or state-owned FIs to participate. This can be a lengthy and highly political process and unless clear benefits for all parties can be demonstrated, may prohibit KYC utilities from developing in some countries.

However, usually, as financial systems develop, customer retention is more closely linked with the quality of differentiable services. Although in more advanced markets, many banks no longer see KYC/AML/data management as a core competency that should remain in-house, in many markets this is not yet the case.

In the EU, the new General Data Protection Regulation (GDPR) has shifted the ownership of data away from firms and back to individuals. In this case, the data are owned by the individuals, not the FI, and a KYC utility would require individuals' permission in order to share their data. This kind of regulation might make utilities much easier to implement since existing incumbency advantage has been wiped-out with the stroke of a pen, and individuals need a better way to manage their identities across multiple independent databases—thereby creating stronger incentives to adopt a KYC utility.

ABOUT IFC AND KYC UTILITIES

IFC has relationships with over 800 FIs globally, including some of the largest global correspondent banks, and some of the smallest microfinance operations in the smallest and most challenging countries. IFC also has a network of IFIs and donors it works with to mobilize advisory support and undertake innovative development projects in difficult markets. IFC is active in the fintech space, has expertise in KYC and AML in-house, and regularly conducts AML and cybersecurity due diligence reviews as part of its risk assessment process. IFC collaborates with the World Bank in every country, and coordinates on KYC/AML issues with the IMF.

The Way Forward

The potential benefits of setting up a KYC utility—less crime, improved data quality, increased inclusion, and greater efficiencies—may far outweigh the costs and complexities, which suggests that the idea merits further exploration and analysis. However, because each country is different, and because each issue discussed in this note must be addressed in each market, we believe the best way to further explore this concept is to pilot a KYC utility in one or two markets facing critical KYC/CDD challenges. Such pilots could help conduct "proof of concept evaluations" that refine the thinking and approach so that KYC utilities are more broadly applicable across markets.

ABOUT THE AUTHORS

Manuela Adl, is a Senior Manager, Financial Institutions Group, IFC. (madl@ifc.org)

William Haworth was Chief Strategy Officer, Financial Institutions Group, IFC, between 2008 and 2017. Prior to joining IFC, he worked for several major consulting firms dealing with financial sector development, institutional restructuring, and privatization. He has worked globally on institutional reform and performance improvement in commercial banking, capital markets, and central bank supervision. He is currently a consultant with IFC. (whaworth@ifc.org)

ACKNOWLEDGMENTS

The authors would like to thank the following colleagues for their review and suggestions: Emile J. M. Van der Does de Willebois, Lead Financial Sector Specialist and Global Lead for Financial Markets Integrity, Global Practice: Finance, Competition and Innovation, World Bank; Harish Natarajan, Lead Financial Sector, Financial Inclusion and Infrastructure, Global Practice: Finance, Competition and Innovation, World Bank; Annetta Cortez, Managing Director, ACT Consulting; Margarete Biallas, Senior Operations Officer, Advisory Services – Digital Financial Services, Financial Institutions Group, IFC; Robert Paul Heffernan, Senior Investment Officer, Financial Institutions Group, IFC; Susan Starnes, Senior Strategy Officer, Sector Economics and Development Impact – Financial Institutions Group, Economics and Private Sector Development, IFC; and Thomas Rehermann, Senior Economist, Thought Leadership, Economics and Private Sector Development, IFC.

Please note the following related EM Compass Notes: *Mitigating the Effects of De-Risking on Remittances* (Note 22); *De-Risking by Banks in Emerging Markets – Effects and Responses for Trade* (Note 24); *How Fintech is Reaching the Poor in Africa and Asia: A Start-Up Perspective* (Note 34); *Can Blockchain Technology Address De-Risking in Emerging Markets?* (Note 38). *Digital Financial Services: Challenges and Opportunities for Emerging Market Banks* (Note 42); *Blockchain in Financial Services in Emerging Markets - Part I: Current Trends* (Note 43); *Blockchain in Financial Services in Emerging Markets - Part II: Selected Regional Developments* (Note 44).

---

1 The term "financial intermediary," or FI, refers to a variety of financial institutions such as universal banks, investment banks, private equity funds, venture capital funds, microfinance institutions, and leasing and insurance companies, among others.

2 Volk, Ariane, Susan Starnes and Michael Kurdyla. 2018. "Increased Regulation and De-risking are Impeding Cross-Border Financing in Emerging Markets." EM Compass Note 48, IFC, Washington, D.C. See also: Starnes, Susan, Michael Kurdyla, Arun Prakash, Ariane Volk, and Shengnan Wang. 2017. "De-Risking and Other Challenges in the Emerging Market Financial Sector: Findings from IFC's Survey on Correspondent Banking." IFC, Washington, D.C.

3 Definition "Correspondent Bank": A Correspondent is a financial institution: (1) that has authorized a Reserve Bank to settle Debit and Credit Transaction Activity to its Master Account for a Respondent or for any financial institution for which the Respondent acts as Correspondent; or (2) that maintains required reserve balances for one or more financial institutions in its Master Account. Definition "Respondent Bank" Definition "Respondent": (1) a financial institution that settles Debit and Credit Transaction Activity for some or all of its Reserve Bank transactions in the Master Account of a Correspondent; or (2) a financial institution that maintains its required reserve balances in the Master Account of a Correspondent. Sources: Federal Reserve Bank, fbrservices.org, accessed Oct 9, 2017. https://www.frbservices.org/financial-services/accounting/servicesetup/respondent-correspondent.html

4 From the 3/18 FSB report: "The data, as of mid-2017, reported in the March 2018 (FSB) report shows that the reduction in the number of correspondent banking relationships continued at the global level in the first half of 2017. Changes varied across regions. While the average number of direct relationships between countries started increasing in North America and Eastern Europe, the decline continued in all other regions: the pace of decline slowed in Africa and Oceania, but increased in the Americas (excluding North America), Asia and Europe (excluding Eastern Europe). While there are no "silver bullets," the actions taken to date under the coordinated FSB action plan are intended to reverse the global decline. But to do so, they will need to be followed up by national authorities and the banking industry."

5 ESAAMLG Eastern and Southern Africa Anti-Money Laundering Group. 2017. "Survey Report on De-Risking in the ESAAMGL Region". September 2017. https://www.esaamlg.org/reports/ESAAMLG_survey_reports_on_de%20_risking.pdf

6 Starnes, Susan, et al. 2017.

7 For evidence of the surging compliance costs see the November 29th, 2017 IIF Briefing note titled: "Improving global AML efforts with Technology and Regulatory Reform." In 2016, in the U.S. alone, financial institutions filed two million suspicious activity reports and these reports are growing at a rate of 11% per year. (The equivalent number in the UK was 500,000.) IIF also noted that "80% to 90% of these reports were of no value to law enforcement."

8 See e.g., Banerjee, Shweta. 2015. "Aadhaar: Digital Inclusion and Public Services in India". World Development Report 2016 – Background Paper Digital Dividends. World Bank Group, 2015. http://pubdocs.worldbank.org/en/655801461250682317/WDR16-BPAadhaar-Paper-Banerjee.pdf

9 Nusca, Andrew. 2017. "Equifax Stock Has Plunged 18.4% Since It Revealed Massive Breach." Fortune.com, September 11, 2017. http://fortune.com/2017/09/11/equifax-stock-cybersecurity-breach/