Center on
Regulation and Markets
at BROOKINGS

WORKING PAPER

THE BROOKINGS INSTITUTION | April 2018

Enhancing anti-money laundering and financial access: Can new technology achieve both?

Michael Barr
University of Michigan

Karen Gifford
Special Advisor, Ripple Labs

Aaron Klein
Brookings Institution

Contents

STATEMENT OF INDEPENDENCE

Michael Barr was an advisor to Ripple Labs until 2017 and is a current advisor to NYCA Partners—a venture capital and advisory firm focused on applying innovation in financial services into the global financial system. Karen Gifford is current advisor to Ripple Labs. Both Gifford and Barr also advise the Global ID Fund. Outside of these affiliations, the authors did not receive financial support from any firm or person for this article or from any firm or person with a financial or political interest in this article. They are currently not an officer, director, or board member of any organization with an interest in this article.

ABOUT THE PAPER

This is a working paper.

Remittances and New Technology

Advances in both private-sector financial technology (FinTech) and technology supporting public sector regulatory compliance (RegTech) offer tremendous promise for broadening and strengthening the global financial system.[1] By vastly reducing the cost of providing financial services, FinTech makes greatly expanded and sustainable financial inclusion a realistic goal. At the same time, greater automation, simplified operational processes, and more detailed and less costly analytics create the potential to enable enhanced transparency while maintaining or improving personal privacy and security of financial activity. Such transparency would in turn support improved financial regulation and supervision as well as consumer protection.

Global financial standard-setting bodies (SSBs) are alive to the opportunity to encourage regulators to harness the strongest capabilities of these new technologies.[2] Doing so would enable financial services providers to create the efficiencies necessary to provide meaningful financial access to the underserved while enhancing anti-money laundering (AML), combating of financing of terrorism (CFT) and other risk mitigation objectives. If done appropriately, FinTech and RegTech would also strengthen regulatory and supervisory capabilities and lower compliance costs. This can be a classic win-win.

Standard-setters, regulators, and global organizations are making positive statements about new technology and are reaching out to FinTech providers to understand technologies better.[3] At the same time, current global financial standards and practices actually impair the adoption of new technology, not least due to uncertainty regarding how these standards, designed with legacy technology in mind, apply to the new capabilities and processes that come with technological advances. There is a significant opportunity to advance efficiency, consumer empowerment, safety and soundness, and anti-money laundering and anti-terrorist financing goals together.

In this paper, we focus on those global standards that apply to cross-border payments. Global financial standards have a large impact on cross-border payments as the challenges regarding interpretation and application of international standards at a national level are amplified by the number of jurisdictions affected. Navigating differing regulatory views and capabilities across jurisdictions is a costly and uncertain venture, confining it to the largest FinTech providers with sufficient funds to negotiate national complexities jurisdiction by jurisdiction. As a result, this is an area where coordinated global action could be especially beneficial. In particular, by encouraging global coordination and appropriate adoption of new technologies, modernized global financial standards could make a substantial contribution to resolving the challenges that currently beset the global remittance market. Apart from being a particularly challenging market, the socio-economic importance of the remittance market also strengthens its bid for priority attention. Remittances represent a key financial service for the growing migrant, refugee, and transnational community who rely on them to remit funds back to their loved ones in their country of origin. Indeed, the G20, the IMF and others working on financial policy have identified remittances as one of the best potential areas of focus for financial inclusion efforts.[4]

We briefly outline the current state of cross-border payments and the challenges it poses for financial access and effective AML/CFT efforts.[5] We discuss recent efforts to ameliorate the shortcomings of the system and discuss the increasing need for global coordination if significant progress is to be made. We make a number of specific recommendations for updating global financial standards to support innovation as a means to enhance financial inclusion, improve transparency, and financial deepening in support of economic growth.

The Cross-Border Payment System Is a Stumbling Block for Both Financial Inclusion and Combatting Money Laundering and Terrorist Financing.

Policy makers across the world have devoted years of effort and study to two high priority goals: improving financial access and combating money launderers and terrorists. While inroads have been made in both areas, progress remains unacceptably slow, especially in the area of cross-border payments.

The current system for global funds transfers is based on old and outdated technology, employed primarily by a shrinking network of correspondent banks.[6] Payments moving through the correspondent banking system are handled by multiple intermediaries, most of which are unaware of the identity of the others. Indeed, the path a cross-border payment will take as it moves around the globe is usually not known to any of the participants in advance. The opacity and uncertainty inherent in such a system provides myriad opportunities for undetected operational failures or intentional manipulation. Many significant AML/CFT prosecutions and enforcement actions of the past 10 years have arisen out of conduct designed to obscure identifying information as a payment moved through the payment chain.[7] The costs inherent in operating a system of this operational complexity and opacity present huge challenges for making services like remittances more affordable for underserved populations. The high risk inherent in the market as it currently functions renders it unattractive to potential providers who are more risk-averse. The lack of competition further contributes to the high costs of remittances.

Risk-Based Approach and De-Risking Responses

The correspondent banking system has been deeply affected by both rising compliance expectations and industries' continuing dependence on aging payments technology. Increasingly since the 1970s, and accelerating after 9/11, policy makers and those in law enforcement have insisted that banks better understand the nature, source and destination of payments moving through their accounts, including the true sender and recipient of the funds involved.

While such an expectation may be quite sound, it can be difficult and expensive for a bank in the correspondent network to determine the nature of the funds it is passing on to another participant bank. Because the system relies on a network of global banks to move funds on behalf of others, a participant bank often has no direct relationship with either the customer sending or receiving a particular payment. Since many

banks have been reluctant to take on the expense of upgrading their international payments infrastructure, most of which dates from the 1980s or earlier, granular analysis of payments data generally involves multiple manual processes, making detailed inquiries cumbersome, costly, and insufficiently effective at catching bad actors.

In terms of the current system, banks place heavy reliance on the risk management abilities of correspondents in the banking remittance network. Increasing sensitivity to the risks of correspondents that may not be able to mitigate the relevant risks to the standards required by the bank have led to the practice of correspondent "de-risking." De-risking refers to the large-scale practice of banks terminating relationships with counterparties and classes of customers, and even exiting entire countries or regions in an effort to limit compliance risk and its attendant costs. The de-risking phenomenon has to be viewed in the context of the mandatory risk-based approach to AML/CFT.

Concerns about the need to limit and direct compliance spending led to the adoption of a mandatory risk-based approach to AML/CFT by the Financial Action Task Force (FATF) in 2012. This approach was intended to shift compliance resources to higher risk areas and, simultaneously, to increase financial inclusion[8] of lower risk customers. Costs and barriers to inclusion could be limited by creating exemptions from the AML/CFT regime where risks were assessed as low and by allowing simplified due diligence where risks were lower, for example in relation to small value payments in jurisdictions with low crime and minimal terrorist financing risks.

Regulators and financial institutions in developing countries have been cautious to make use of the space to simplify due diligence,[9] especially as they are hesitant to run afoul of international assessors of compliance with the FATF standards. Important steps have nevertheless been taken by countries such as India, Pakistan, Nigeria and Uganda to simplify AML/CFT due diligence in lower risk cases.[10] Such steps are, however, largely confined to domestic financial services. Little has yet been done to move forward on simplifying or improving due diligence in relation to cross-border remittances as that requires an alignment between the risk assessments and risk approaches of the relevant national regulators and their foreign counterparts.

The increased focus on risk, combined regulatory uncertainty, with very large fines for non-compliance levied in the US and UK, and concerns about profitability of business lines, have led to a post-2012 cycle of de-risking.[11] The Committee on Payments and Market Infrastructure (CPMI) summarized this cycle as follows: "increasing costs, regulatory pressure and an increased perception of risk are reducing the profit margins associated with this activity in some countries and/or with some customers and could be making [cross-border payment services] increasingly unappealing to a growing number of correspondent banks."[12] In the same report, the CPMI noted that the "threat that cross-border payment networks might fragment and that the range of available options for these transactions could narrow" is real and growing.[13]

As part of the current cycle financial institutions began employing risk-based principles to re-examine customer relationships, asking whether particular customers generate sufficient income to justify additional compliance investments. Firms undertaking this analysis increasingly have chosen to terminate or restrict business relationships with remittance companies and smaller local banks in certain regions of the world. Those most vulnerable in the de-risking cycle are the low margin customers, not necessarily high-risk, high-value customers. This is because risky customers that generate substantial fees often prove more

attractive than less profitable customers with lower risk, even when the high-risk customers require expensive monitoring.[14]

Frustratingly for policy makers, therefore, the victims of de-risking cycles are disproportionately lower income migrant workers attempting to send money to family members in their home countries, as opposed to higher-risk potential bad actors who launder money or finance terror.

Concerned about de-risking, FATF and national regulators issued statements calling on banks not to engage in large-scale de-risking terminations. The Financial Stability Board is also working jointly with the World Bank, the CPMI and FATF on a four-point plan to (i) deepen their understanding of the extent and impact of these terminations, (ii) provide increased regulatory clarity, (iii) support AML/CTF capacity building in affected low capacity countries, and (iv) harness technology to improve customer due diligence measures of correspondent and respondent banks. While these objectives are sound, no compelling evidence has yet emerged that these measures have reversed the de-risking cycle.

Current Pressures May Be Making an Opaque System Worse

Notwithstanding the toll that AML/CFT-related de-risking has taken on those seeking to access the global financial system for legitimate purposes, the current system of cross-border payments continues effectively to provide cover for bad actors who benefit from its inherent lack of transparency. Moreover, recent de-risking cycles may have the effect of increasing barriers to detection of money laundering and terrorist financing. The Global Center on Cooperative Security found that "[r]ather than reducing risk in the global financial sector, de-risking actually contributes to increased vulnerability by pushing high-risk clients to smaller financial institutions that may lack adequate AML/CFT capacity, or even out of the formal financial sector altogether."[15]

Technological Innovation Holds Promise for Risk Reduction and Greater Inclusion, But Faces Regulatory Barriers to Adoption

The Promise of FinTech Innovation

Solutions to these problems are being developed. As the International Monetary Fund recently reported, "[t]he area of cross-border payments is especially ripe for change, and could benefit from new technologies."[16] Technological advances with the potential to lower radically the costs and risks associated with cross-border payments are developing at a furious pace.

A number of new innovations directly address well-known cross-border payment risks. One such risk, the danger that a payment will fail on its way through the correspondent banking network (sometimes referred to as Herstatt risk) can be eliminated by technologies that enable direct, point-to-point settlement of cross border payments.[17] Addressing this risk in turn obviates the need for many operational processes embedded in the current cross-border payment system, all of which raise the cost and slow the pace of international payments.

Reducing cost and time of international payments has the potential to vastly invigorate financial inclusion efforts. To date, many such efforts have sought to move forward primarily on a charitable basis, meaning that they are often unsustainable without substantial ongoing outside funding. Changing the cost structure for payments via increased automation can transform those who are financially excluded into potentially valuable customers for new financial products and services. Indeed, after exploring a number of alternatives, the Gates Foundation's Financial Services for the Poor initiative concluded that "the most effective way to significantly expand poor people's access to formal financial services is through digital means."[18]

FinTech innovation also offers the promise of improved transparency and security in cross-border payments. Greater automation of the cross-border payments process itself offers significant benefits in this area, as more and better automation could simplify the payments path, bypassing the current correspondent banking system. Doing so could greatly reduce the number of manual steps necessary to effect a cross-border payment, and the consequent opportunity for error or illegality to occur.

Innovations such as portable digital identity offer additional promise for both lowering the cost of delivering financial services and improving financial transparency.[19] While several portable digital identity frameworks have been articulated, and quite a number of digital identity products and services are in development, most share the following characteristics: identity details are collected only once and held or controlled by the individual to whom they relate, enabling that person to share identity details with various entities as needed to obtain financial services.[20] This system stands in contrast with current practice, where identity details must be gathered separately by each service provider, which then holds the data for all of its customers, a repetitive and expensive process, and one that provides a convenient attack point for nefarious actors seeking to steal financial data.

Under the current cross-border payments regime, payment traceability is constrained because customer information is held at individual financial institutions. Thus, when payments move through multiple institutions, it can be difficult or impossible to connect an ongoing payment with its true origin, or with the identity information of the original sender or ultimate recipient. At the same time, the fact that personal information is held and replicated at multiple financial institutions increases the opportunity for security breaches and data theft. Identity portability offers the possibility that payments information could be traced globally, rather than remaining confined within silos managed by financial institutions.

FinTech also offers the benefit of more effective collaboration between financial institutions and law enforcement agencies. Money laundering and terrorist financing risks are in essence national security and law enforcement risks. The correct identification, assessment and management of these risks are heavily dependent on sensitive intelligence that governments generally do not share with financial institutions. Financial institutions therefore find it particularly difficult to combat money laundering and terrorist financing efficiently. New technology, especially new data technology, provides platforms for secure and

meaningful public-private collaboration in this regard, while preserving privacy and commercial confidentiality.[21]

Policy Responses to Innovation Often Favor Established Players

While new FinTech developments are appearing at a rapid pace, access to the global financial system is not expanding in correspondence with this wave of innovation.[22] Regulatory issues play an outsized role in the friction slowing the adoption of new technology. In many cases, it is hard to evaluate how new technologies square with standards written with older technologies in mind, and this regulatory uncertainty creates a barrier to new adopters and favors established players over new entrants. Even worse, in practice compliance with some standards require FIs to resort to manual processes, creating roadblocks for the adoption of new more automated technology that could solve longstanding problems better, faster, and at a lower cost.[23]

While individual countries and even some regions have undertaken useful initiatives to support responsible adoption of FinTech solutions, at the global level, where cross-border payments are most strongly affected, policy response to new technology has been muted. Why has this been the case? We see a number of factors that appear to be playing a role:

- **Strong focus on risks of new technology.** Policy makers' training is to protect the financial system from risk - and the potential for risk is quite clear when a new product or technology comes on line. As a result, policy makers expend great effort to mitigate risk presented by new technologies. Then director of United States Financial Crimes Enforcement Network (FinCEN) expressed a reaction to FinTech innovation that is common among financial regulators, emphasizing only the dangers it presents: "These new systems have also expanded the boundaries of "money transmission" as more sophisticated payment systems have become available. And the inherent added complexity of these systems opens them to potential misuse by criminals. FinCEN's analysts are continually working to understand the schemes and methods used to exploit emerging payment methods for money laundering and terrorist financing, and to develop related guidance for law enforcement."24

  While the effort to understand and mitigate risks posed by new technologies is appropriate and necessary, there is a need for corresponding efforts to understand the risks associated with continued use of aging technology for cross-border payments, and for the ability of innovative technology to reduce systemic and AML/CFT risks, not just exacerbate them.

- **Regulatory framework shaped by legacy systems and technologies.** Current financial policies and regulations reflect the legacy systems and technologies that were in place at the time they were created.25 These requirements were designed to ameliorate the particular risks presented by a payments system running on technology that dates from the 1980s or earlier - in which most cross-border transactions take days or even weeks to settle, traveling over opaque pathways via multiple intermediaries which are unknown to the sender and receiver in advance. In this circumstance, requirements for repeated screening and transaction monitoring entailing multiple manual interventions may be warranted.

As discussed above, the need for repetitive manual monitoring of individual transactions could potentially be obviated through the use of a number of innovative technologies; however, regulators and industry participants may be reluctant to explore the functionalities of such technologies when there are concerns whether these would meet global financial standards. SSBs can and should take action to clarify the conditions under which financial institutions should be allowed or even encouraged to make appropriate use of new technologies to address risk in effecting cross-border payments.

- **Ghettoizing financial inclusion efforts.** Policy makers in financial services traditionally treated financial inclusion as a "nice to have," but not core to their central mission of ensuring the strength of the global financial system. Despite growing recognition that financial exclusion poses concrete risks to the system—including enabling money laundering and terrorist financing, higher costs borne among those least able to afford them, greater crime domestically and abroad, and lower economic growth—this view continues to influence policymakers, in ways both acknowledged and unacknowledged.

  We believe that financial inclusion is a key part of ensuring financial growth, stability, and fighting crime and terrorism. This links with the recognition of the interdependence of the financial policy objectives of financial inclusion, stability, integrity, and consumer protection in the terms of reference of the G20s Global Partnership for Financial Inclusion.26 We believe that FinTech can contribute greatly to the advancement of all four objectives. For that benefit to realize, however, a better and clearer alignment is required among the different sets of SSB standards. For example, as noted earlier, the FATF has repeatedly issued guidance informing a risk-based approach to AML/CFT compliance, most recently with renewed and expanded guidance in November 2017. It explicitly permits regulators to exempt certain classes of entities from specific AML/CFT obligations in what it terms "proven low-risk scenarios".27 It is unclear, however, how such an exemption would square with other standards that are not directly geared toward financial inclusion.28

  Rather than tolerating lowered standards under specified situations, SSBs have an opportunity to raise standards across the board and encourage industry to modernize. FinTech and improved identification technology may, for example, simplify customer identification processes to such an extent that there may be little need or appetite for identification exemptions or for simplified customer due diligence that is only focused on lower risk scenarios. Creating a standards framework that encourages modernization and the use of the best technology can and will offer permit all financial system participants to benefit from new developments that are able to addresses longstanding operational and compliance risks in cross-border payments and increase effectiveness and efficiency across the board.

Proposed Solution: Enhanced Uniform Standards for Cross-Border Payments

We propose that SSBs come together in a focused effort to create a joint new cross-border payment standard, one that is tech-neutral—agnostic as to particular technological solutions—but tech-focused—enabling new technology to be used both to transmit funds and to catch bad actors. One model SSBs could draw on in shaping a coordinated effort is the U.S. Federal Financial Institutions Examination Council (FFIEC), the interagency council that is "empowered to prescribe uniform principals, standards, and report forms" for the U.S. federal government's examination of financial institutions, which is conducted by multiple bank regulators.[29]

Updated standards should enable new technology to be harnessed responsibly; i.e., further both inclusion and AML/CTF efforts. New guidance should take advantage of new technological developments that directly address common payments risks in the cross-border setting.[30] Relevant new capabilities include point-to-point payments and portability of identity. Possible new requirements that spring from these capabilities include:

Require settlement for cross-border payments in a specified, shorter time frame (same day or faster). A number of technologies currently enable same-day settlement domestically or regionally. Expanding the requirement for same day settlement to the cross-border context would represent a substantial advance for both inclusion and AML/CFT goals. As noted above, current rules permit much longer timeframes for settlement of cross-border payments, which provide bad actors with greater opportunities to interfere in legitimate transactions, changing information and flows of funds to cover tracks. Further, longer delays in settlement impose costs on those transmitting the funds, particularly lower income and more vulnerable populations. Multiple nations (for example the U.K., Poland and Mexico) have adopted real or near real-time payment systems for transactions within their borders. Other nations, notably the U.S., continue to allow slow domestic payment systems (at substantial costs to their own citizens, particularly those of lower incomes).[31] Given the prevalence of faster payments and the stated objective of most nations to achieve faster payments, SSBs should emphasize faster payment and settlement times as a global priority.

Require pre-confirmation of the recipient account. Pre-confirmation would vastly reduce the opportunity for operational failures and fraud. In addition, pre-confirmation would support other regulatory compliance measures such as pre-disclosure of transaction fees, something that legacy technology currently in place does not support. In order for a competitive market to take place, the sender must know the full cost of the transaction. This can best be expressed as the amount that the recipient will receive in the local currency of receipt. This requirement was put into place in the United States in the Dodd-Frank Act for low dollar remitters and can and should be incorporated into global standards.

Require interoperability of payment systems. Interoperability of national payment systems would greatly further the goal of lowering the cost and improving the speed of global payments, two essential pre-requisites for meaningful and sustainable financial inclusion efforts in the cross-border context. A number of countries have begun to require interoperability between domestic payments systems.[32] Even

among countries that have lagged in updating their payment systems, such as the United States, there has been a recognition that interoperability is a critical step needed in modernizing payment systems.[33]

Require portability of identity. Identity portability offers a number of benefits, including eliminating a significant barrier to entry for new service providers and creating the possibility for greatly enhanced financial system transparency. Enabling individuals to own their identity details in digitized form offers the possibility of enhancing personal privacy and information security. In addition, portable digital identity supports financial inclusion efforts by reducing or eliminating expensive and repetitive data collection efforts associated with customer on-boarding. The European Union has taken important steps to support portable identity. Portability of identity for the purpose of accessing financial services should be a global standard.

Standards should encourage adoption of new technology while allowing countries and participants to adopt at varying paces. Given the unique nature of the global payment system it is unrealistic to expect uniform technologies or even a uniform pace of adoption. SSBs should allow for differing rates and forms of adoption. Indeed, some experimentation of different technologies may be optimal as data are thus created to allow comparisons of effectiveness. However, one option that should not be allowed to continue is the status quo. SSBs should create a timeline for changes in terms of action and adoption of certain principles, without overly proscribing exact technologies or specific deadlines (e.g. how many milli-seconds to hours constitutes 'real-time' for payments, or whether block-chain or database systems should be used).

Conclusion

SSBs have a unique opportunity to shape the evolving financial system. Now, at a time when both established players and new entrants to the financial system are beginning to adopt new FinTech solutions, guidance that encourages greater transparency and inclusion can have a powerful opportunity to shape and speed up adoption processes.

Failing to act poses significant dangers. Uncertainty leaves constructive players stymied, and effectively provides bad actors with an advantage. Delays, excessive fees and diminishing access to remittance services cause individual hardship, impede humanitarian efforts, threaten economic disruption, and reduce progress on financial inclusion. They provoke remitters to seek and use non-mainstream methods of sending funds, which in effect provide greater ability for bad actors to piggy-back and transmit money globally avoiding detection.

Moreover, while disproportionately harming the underserved, uncertainty in the realm of cross-border payments has broader ramifications. Financial institutions wary of changing to new technology spend more on each transaction, reducing their incentive to compete and bring in new customers. To the extent costs are averaged across customers, non-users of international money transmission pay more in higher bank fees. Innovators seeking to serve cross-border markets are unable to compete as the de-risking cycle reduces access to financial institutions for money transmission businesses. AML/CTF objectives are not met as illicit

funds are able to move more easily, masked by either larger flows outside of financial institutions by migrants, or by slower, lower technological processes by which financial institutions move funds. Looking for the real needle in the haystack gets harder when either fake needles or more hay is added.

The best way for SSBs to ensure that new technology fulfills its highest promise is to bring FinTech within regulatory purview. SSBs are uniquely well positioned to do this with respect to cross-border payments, bringing global payment system into the 21st century. No single country's efforts, however forward-thinking they may be, can accomplish this. By acting in a coordinated manner, developed financial countries can expand financial inclusion while promoting new technologies that will enhance capacity to meet AML and anti-terrorism goals.

References

Artingstall, David et al. (February, 2016), Drivers & Impacts of Derisking. *John Howell & Co. Ltd*. Retrieved from https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf

Banque de France (April, 2016), Financial Stability in the Digital Era. *Digital Stability Review, Banque de France*. Retrieved from https://publications.banque-france.fr/sites/default/files/medias/documents/financial-stability-review-20_2016-04.pdf

Basel Committee on Banking Supervision (May, 2009), Due diligence and transparency regarding cover payment messages related to cross-border wire transfers. *Bank for International Settlements*. Retrieved from https://www.bis.org/publ/bcbs154.htm

Basel Committee on Banking Supervision (June, 2017), Sound management of risks related to money laundering and financing of terrorism. *Bank for International Settlements*. Retrieved from https://www.bis.org/bcbs/publ/d405.pdf

Baer, Greg (28 June, 2017), Testimony of Greg Baer, Examining the BSA/AML Regulator Compliance Regime. *The Clearing House*. Retrieved from https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-gbaer-20170628.pdf

Bill & Melinda Gates Foundation (2017), Financial Services for the Poor Strategy Overview: The Opportunity. *Bill & Melinda Gates Foundation*. Retrieved from https://www.gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor

Calvery, Jennifer Shasky (16 April, 2013), Remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network. *United States Department of Treasury*. Retrieved from https://www.fincen.gov/news/speeches/remarks-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-4

Cassara, John (18 July, 2017), Managing Terrorism Financing Risk in Remittences and Money Transfers. *House Committee on Financial Services*. Retrieved from https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-jcassara-20170718.pdf

Charity Finance Group (March, 2015), Briefing: Impact of banks' de-risking on Not for Profit Organizations. *Charity Finance Group*. Retrieved from http://www.cfg.org.uk/Policy/~/media/Files/Policy/Banking/Briefing%20%20Impact%20of%20banks%20derisking%20activities%20on%20charities%20%20March%202015.pdf

Council of Europe (September, 2017), Anti-money laundering and counter-terrorist financing measures. *Council of Europe*. Retrieved from https://rm.coe.int/andorra-fifth-round-mutual-evaluation-report/168076613e

De Koker, Singh and Capal 'Closure of bank accounts of remittance providers: Global challenges and community perspectives in Australia' 2017 *University of Queensland Law Journal* 119 149.

Decentralized Identity Foundation (2017). The Pillars of a New Ecosystem. *Decentralized Identity Foundation*. Retrieved from http://identity.foundation

Department of Justice ABM Amro Bank Case (10 May, 2010), Former ABN Amro Bank N.V. Agrees to Forfeit $500 Million in Connection with Conspiracy to Defraud the United States and with Violation of the Bank Secrecy Act. *Department of Justice, Office of Public Affairs*. Retrieved from https://www.justice.gov/opa/pr/former-abn-amro-bank-nv-agrees-forfeit-500-million-connection-conspiracy-defraud-united

Department of Justice (18 August, 2010), Barclays Bank PLC Agrees to Forfeit $298 Million in Connection with Violations of the International Emergency Economic Powers Act and the Trading with the Enemy Act. *Department of Justice, Office of Public Affairs*. Retrieved from https://www.justice.gov/opa/pr/barclays-bank-plc-agrees-forfeit-298-million-connection-violations-international-emergency

Department of Justice Commerzbank AG Case (12 March, 2015), Commerzbank AG Admits to Sanctions and Bank Secrecy Violations, Agrees to Forfeit $563 Million and Pay $79 Million Fine. *Department of Justice, Office of Public Affairs*. Retrieved from https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and

Department of Justice BNPP Case (01 May, 2015), BNP Paribas Sentenced for Conspiring to Violate the International Emergency Economic Powers Act and the Trading with the Enemy Act. *Department of Justice, Office of Public Affairs*. Retrieved from https://www.justice.gov/opa/pr/bnp-paribas-sentenced-conspiring-violate-international-emergency-economic-powers-act-and

Durner, Tracey and Shetret, Liat (November 2015). Understanding Bank De-Risking and Its Effects on Financial Inclusion. *Global Center on Cooperative Security*. Retrieved from http://www.globalcenter.org/wp-content/uploads/2015/11/rr-bank-de-risking-181115-en.pdf

Erbenova, Michaela et al. (30 June, 2016). The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action. *International Monetary Fund*. Retrieved from http://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/The-Withdrawal-of-Correspondent-Banking-Relationships-A-Case-for-Policy-Action-43680

Faster Payments Task Force (July, 2017), The U.S. Path to Faster Payments Final Report Part Two: A Call to Action. *Faster Payments Task Force*. Retrieved from http://fasterpaymentstaskforce.org/wp-content/uploads/faster-payments-task-force-final-report-part-two.pdf

FATF (2013-2017), Anti-money laundering and terrorist financing measures and financial inclusion - With a supplement on customer due diligence, *FAFT, Paris*. Retrieved from www.fatf-gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

FFEIC (01 September, 2017), About the FFIEC. *Federal Financial Institutions Examination Council*. Retrieved from https://www.ffiec.gov/about.htm

Finance and Markets Global Practice of the World Bank Group (October, 2015), Report on the G20 Survey on De-Risking Activities in the Remittence Market. *The World Bank Group*. Retrieved from http://documents.worldbank.org/curated/en/679881467993185572/pdf/101071-WP-PUBLIC-GPFI-DWG-Remittances-De-risking-Report-2015-Final-2.pdf

Finance and Markets Global Practice of the World Bank Group (November, 2015), Withdrawal from Correspondent Banking; Where, Why, and What to Do About It. *International Bank for Reconstruction and Development / The World Bank Group*. Retrieved from http://documents.worldbank.org/curated/en/113021467990964789/pdf/101098-revised-PUBLIC-CBR-Report-November-2015.pdf

Global ID (2017). *Global ID*. Retrieved from https://www.globalid.net

Global Partnership for Financial Inclusion *Global Standard-Setting Bodies and Financial Inclusion - The Evolving Landscape* (2016) 6.

Global Standards Proportionality Working Group (August, 2016). Stemming the Tide of De-Risking Through Innovative Technologies and Partnerships. *Alliance for Financial Inclusion*. Retrieved from https://www.afi-global.org/sites/default/files/publications/2016-08/Stemming%20the%20Tide%20of%20DeRisking-2016.pdf

He, Dong (01 November, 2017), Fintech and Cross-Border Payments. *International Monetary Fund*. Retrieved from https://www.imf.org/en/News/Articles/2017/11/01/sp103017-fintech-and-cross-border-payments

Hopper, Robert (2016), Disconnecting from Global Finance. *The Commonwealth*. Retrieved from http://thecommonwealth.org/sites/default/files/inline/DisconnectingfromGlobalFinance2016.pdf

Howes, David (05 September, 2016), Halting the decline of correspondent banking. *Sibos*. Retrieved from https://www.sibos.com/media/news/halting-decline-correspondent-banking

Keatinge, Tom (2014), Uncharitable Behavior, *Demos*. Retrieved from https://www.demos.co.uk/files/DEMOSuncharitablebehaviourREPORT.pdf

Klein, Aaron (28 September, 2016), Why don't checks clear instantly? Ask the Fed. *Politico*. Retrieved from https://www.politico.com/agenda/story/2016/09/financial-technology-payment-transactions-federal-reserve-000209

Klein, Aaron (17 March, 2016), Why Do 1970s Prices Dictate Anti-Money Laundering Rules?. *Bipartisan Policy Center*. Retrieved from https://bipartisanpolicy.org/blog/1970s-prices-anti-money-laundering/

Koblanck, Anna (2015), Achieving Interoperability in Mobile Financial Services, Tanzania Case Study. *International Finance Corporation. Retrieved from* https://www.ifc.org/wps/wcm/connect/8d518d004799ebf1bb8fff299ede9589/IFC+Tanzania+Case+study+10_03_2015.pdf?MOD=AJPERES

Lowery, Clay and Ramachandran, Vijaya (09 November, 2015). *Unintended Consequences of Anti-Money Laundering Policies for Poor Countries*. Retrieved from https://www.cgdev.org/publication/unintended-consequences-anti-money-laundering-policies-poor-countries

Migration and Remittances Team, Development Prospects Group, World Bank (13 April, 2015). Migration and Remittances: Recent Developments and Outlook Special Topic: Financing for Development. *The World Bank*. Retrieved from https://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief24.pdf

Scott, Paul, et al. (19 February, 2015), Hanging by a Thread: The ongoing threat to Somalia's remittence lifeline. *Adeso*. Retrieved from https://policy-practice.oxfam.org.uk/publications/hanging-by-a-thread-the-ongoing-threat-to-somalias-remittance-lifeline-344616

Taylor, Argus (5 October, 2017), National digital ID to go public. *Innovation Australia*. Retrieved from http://www.innovationaus.com/2017/10/National-digital-ID-to-go-public?utm_content=61363818&utm_medium=social&utm_source=twitter

Warden, Staci (July, 2015), De-Risking and Its Consequences for Global Commerce and the Financial System. *Milken Institute*. Retrieved from http://assets1c.milkeninstitute.org/assets/Publication/Viewpoint/PDF/De-Risking-CBR-Summary-Report-Formatted-v4.pdf

The Windhover Principles for Digital Identity, Trust, and Data (2017). *Institute for Data Driven Design*. Retrieved from https://idcubed.org/home_page_feature/windhover-principles-digital-identity-trust-data/

The World Bank (05 April, 2017), Financial Inclusion Overview. *The World Bank*. Retrieved from http://www.worldbank.org/en/topic/financialinclusion/overview

Notes

1. We employ the term "FinTech" to refer to new technology and innovation that enables the delivery of financial services. Examples of FinTech include the use of mobile phones for the delivery of financial services and the use of cloud computing, application programming interfaces (APIs), open protocols, enhanced data storage, analysis and management capabilities to reduce the time and cost of financial transactions.
2. The six SSBs include the Basel Committee on Banking Supervision (BCBS), the Committee on Payments and Market Infrastructures (CPMI), the Financial Action Task Force (FATF), the International Association of Deposit Insurers (IADI), the International Association of Insurance Supervisors (IAIS), and the International Organization of Securities Commissions (IOSCO).
3. See for example, IMF, "Fintech and Financial Services: Initial Considerations," Staff Discussion Notes, June 19, 2017.
4. GPFI guidance note, IMF paper, CPMI 2016 report-guiding principle 7
5. Cross-border payments raise a large number of policy issues. In this limited paper we restrict our scope to those aspects of the global payment system that could be considered infrastructural: customer identification and authentication, and the settlement process itself. Infrastructural issues surrounding cross-border payments represent a relatively contained set of questions, and also present an area where the global policy community is particularly well positioned to make significant advances. While we do not address other important policy areas such as consumer and data protection, including cyber security, our recommendations are informed by our support and sensitivity to these important policy objectives.
6. Howes, Halting the decline of correspondent banking, 2016.
7. Department of Justice ABM Amro Bank Case,10 May 2010; Department of Justice Barclay Case, 18 August, 2010; Department of Justice BNPP Case, 01 May, 2015; Department of Justice Commerzbank AG Case, 12 March 2015.
8. FATF, Revised Guidance on AML/CFT and Financial Inclusion, 2017.
9. CPMI 2016 report, para. 106
10. FATF, Revised Guidance on AML/CFT and Financial Inclusion, 2017.
11. Large global financial institutions are among those most likely to de-risk according to World Bank data, in part because of the lack of consistency among global standards. Ironically, these larger institutions are precisely those with the resources to adopt and implement new technologies on a large scale. As the Milken Institute study De-risking and Its Consequences for Global Commerce and the Financial System found: "A fragmented regulatory environment and conflicting regulations from country to country have added to the lack of clarity. Participants noted that most regulatory decisions are taken without a coordinated approach, and further, that regulations are not consistent across jurisdictions, which is a problem in particular for global financial institutions." For de-risking studies, see for example, Migration and Remittances Team, Development Prospects Group, 'Migration and Remittances: Recent Developments and Outlook' Special Topic: Financing for Development' (Migration and Development Brief No 24, World Bank, 13 April, 2015); Global Standards Proportionality (GSP) Working Group, 'Stemming the Tide of De-Risking through Innovative Technologies and Partnerships' (Discussion paper for the G-24/AFI Roundtable at the IMF and World Bank Annual Meeting, Alliance for Financial Inclusion, 7 October 2016); Centre for Global Development, Unintended Consequences of Anti-money Laundering Policies for Poor Countries (11 September 2015) 10; MONEYVAL Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, 'De-risking' within Moneyval States and Territories' (Report, Council of Europe, 4 April 2015); Tracey Durner and Liat Shetret, 'Understanding bank de-risking and its effects on financial inclusion – An exploratory study' (Research Report, Global Centre on Cooperative Security, November 2015); Scott Paul et al, Hanging by a thread: the ongoing threat to Somalia's remittance lifeline (Oxfam, 2015); David Artingstall et al, Drivers & Impacts of Derisking (John Howell & Co Ltd, 2016); The Commonwealth, Disconnecting from Global Finance De-risking: The Impact of AML/CFT Regulations in Commonwealth Developing Countries (2016); Aledjandro Lopez Mejia et al, 'The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action' (Staff Discussion Note, IMF, 30 June 2016); Tom Keatinge, Uncharitable

behaviour (Demos, 2014) 16; Charity Finance Group, Briefing: Impact of banks' de-risking on Not for Profit Organisations (March 2015). De Koker, Singh and Capal 'Closure of bank accounts of remittance providers: Global challenges and community perspectives in Australia' 2017 University of Queensland Law Journal 119.

12. CPMI, Consultative Report, Correspondent Banking, 2015.
13. Another study by the Milken Institute estimated that since 2012, 200,000 trade-finance lines to Africa have been cut.
14. The World Bank conducted on a survey on de-risking for the G20 in 2015 and found that "[t]he number of [bank] accounts being closed appears to be increasing." Significantly, the number one cited reason for account closure was profitability, not AML/KYC violations.
15. Durner and Shetret, Understanding Bank De-Risking and its Effects, 2015.
16. He, Fintech and Cross-Border Payments, 2017.
17. Gifford and Cheng, "Implementation of real-time settlement for banks using decentralised ledger technology: policy and legal implications," Financial Stability Review No. 20, April 2016, pp. 148-49.
18. The Gates Foundation, 2017.
19. An early articulation of a vision for portable identity, the Windhover Principles for Digital Identity, Trust and Data, articulated by an industry group in 2014, describe how portability of identity might enable a better balance privacy, security and appropriate transparency than is possible using current identity management technology and practices. Since that time a number of real-world efforts have sprung up attempting to actualize identity portability.
20. Examples of portable identity efforts include Aadhar; Nigerian digital identity effort; Australian digital identity effort; Digital Identity Foundation; and globalID.
21. De Koker, Singh and Capal 'Closure of bank accounts of remittance providers: Global challenges and community perspectives in Australia' 2017.
22. The World Bank Financial Inclusion Overview, 2017.
23. See, for example, BCBS, Due diligence and transparency regarding cover payment messages related to cross- border wire transfers (2009) para. 26-28, on the obligation of intermediary banks in the correspondent banking network to conduct sanctions screening even if that screening has been conducted by the originating bank. Sanctions screening inevitably involves manual processes, as red flags are often triggered by misspellings and other identity-related issues that must be cleared though individualized investigations. When these investigations take place midway through the payment stream, they render automation of the payment stream, with its substantial benefits for financial inclusion, impossible. Ironically, they can also provide they kinds of manual interventions in the payment stream that enable operational failure and intentional manipulation of payment-related information.

    Similarly, BCBS's Sound management of risks related to money laundering and financing of terrorism (2017) contains an appendix devoted to management of the risks presented by cross-border payments using the correspondent banking network. While that document does not explicitly require manual or duplicative processes, it does state that banks should institute:

    > appropriate policies and procedures to be able to detect any activity that is not consistent with the purpose of the services provided to the respondent bank or any activity that is contrary to the commitments that may have been concluded between the correspondent and the respondent.

    As a practical matter, this guidance has generally been interpreted to require a transaction-by-transaction assessment of whether payments moving through a correspondent bank are consistent with information provided by the respondent bank. This kind of inquiry is by its nature difficult to undertake via automated processes. The guidance notes that the need for this and other risk management processes required for correspondent banks arises from the limited amount of information correspondent banks possess about the ultimate sender and recipient of the payments in question. Id. at Annex 2 para. 3-4. Technology such as point-to-point payments and portable digital identity could add considerable transparency in this situation.

24. Remarks of Jennifer Shasky Calvery, Director, FinCEN, April 16, 2013.

25. As the Clearinghouse report on AML/CFT regulation finds that it is: "grounded in the analog technology of the 1980s, rather than the more interconnected and technologically advanced world of the 21st century. For example, in the U.S. the two primary sources of data, currency transaction reports (CTRs) and Suspicious Activity Reports (SARs) are based on reporting thresholds that in some instances have not been adjusted since the 1970s.

26. Global Partnership for Financial Inclusion, 2016.

27. FATF, Revised Guidance on AML/CFT and Financial Inclusion, 2017.

28. Subsequent guidance from both FATF and BCBS, while acknowledging the problem of de-risking, makes clear that regulatory expectations for cross-border payments continue to include individualized assessments of particular transactions:

> In a correspondent banking relationship, the correspondent institution will monitor the respondent institution's transactions with a view to detecting any changes in the respondent institution's risk profile or implementation of risk mitigation measures (i.e. compliance with AML/CFT measures and applicable targeted financial sanctions), any unusual activity or transaction on the part of the respondent, or any potential deviations from the agreed terms of the arrangements governing the correspondent relationship. In practice, where such concerns are detected, the correspondent institution will follow up with the respondent institution by making **a request for information (RFI) on any particular transaction(s), possibly leading to more information being requested on a specific customer or customers of the respondent bank.**

FATF, Correspondent Banking Services (2016) para. 3. The guidance specifies that a correspondent bank, in investigating individual transactions, must be able to ask its customer bank about particular transactions that bank's customer, including the bank's customer's sources of funds, whether the customer's transaction history is consistent with its customer profile, whether the customer has any relationship to third parties, and other detailed information. Id. para 32.

The requirements included in these guidelines envision the type of individualized investigation occurring within the payment stream that makes automation impossible. See discussion in note [12] above. Moreover, they would appear to make it impossible for an institution that had availed itself of simplified KYC requirements to access the correspondent banking system, and thus the global financial system itself. FATF, Correspondent Banking Services (2016); BCBS, Sound management of risks related to money laundering and financing of terrorism (2017)

29. About the FFIEC, 2017.

30. For example, as the Center on Sanctions and Illicit Finance recently testified before the United States House of Representatives, "Since many hawaladars and similar underground financial networks often use financial institutions, advanced analytics should be employed to provide the transparency that the hidden systems seek to deny." However, in order for financial service providers to employ these kinds advanced analytics, those analytics must be considered acceptable to the regulator as a means of detection of illicit activity. Further, the data necessary to generate the advanced analytics must be available to the institution employing the analytics. In the world of international payments, this requires standardization on multiple fronts.

31. Klein, Why don't checks clear instantly? Ask the Fed, 2016.

32. Koblanck, Achieving Interoperability in Mobile Financial Services, 2015.

33. Faster Payments Task Force, The U.S. Path to Faster Payments, 2017.

Center on
Regulation and Markets
at BROOKINGS

The Brookings Economic Studies program analyzes current and emerging economic issues facing the United States and the world, focusing on ideas to achieve broad-based economic growth, a strong labor market, sound fiscal and monetary policy, and economic opportunity and social mobility. The research aims to increase understanding of how the economy works and what can be done to make it work better.

Questions about the research? Email communications@brookings.edu.
Be sure to include the title of this paper in your inquiry.