Research Memo

Center on Sanctions & Illicit Finance
FOUNDATION FOR DEFENSE OF DEMOCRACIES

Designing a New Anti-Money Laundering (AML) System

By Juan C. Zarate and Chip Poncy

September 2016

Executive Summary

Over the past 15 years, concerns over the dangerous and corrosive impact of illicit financing have shaped core national security strategies and underscored the importance of defending the integrity of the financial system.[1] The United States government and other authorities have used the tools of financial pressure, sanctions, and regulation to address every major international security concern – from terrorism and nuclear proliferation to kleptocracy and human rights abuses – with a growing demand on the financial community to prevent rogue actors and illicit capital from entering the financial system.

Given the attention, importance, and resources concentrated on the issues of financial integrity and security, this is a critical moment to clarify the purpose of the anti-money laundering/combating the financing of terrorism (AML/CFT) system and ask whether it is working as intended. This question takes on more importance as organizations invest ever-increasing resources into compliance with financial regulations and as greater policy demands are placed on the tools and strategies of financial pressure.

The AML rules and regulations developed over the past four decades were built to facilitate transparency, traceability, and accountability. The modern AML/CFT system is intended to be systemically effective to deter, detect, and disrupt illicit financing, but it cannot stop all illicit activity. The risk-based model upon which the AML/CFT regime relies assumes that not all dirty money will be stopped, nor will every dollar be detected, traced, and seized. No institution or country, however much it spends, can thwart all illicit actors.

Billions of dollars of fines have been levied against banks for failure to comply with AML/CFT requirements, and billions more have been invested by the private sector in compliance systems, personnel, and remediation to meet increasing global standards.

1. This memo appeared originally as: Juan C. Zarate and Chip Poncy, "Designing a New AML System," *Banking Perspectives*, Q3 2016. (https://www.theclearinghouse.org/publications/2016/2016-q3-banking-perspectives/a-new-aml-system) and is derived largely from the keynote address delivered by Juan C. Zarate at the Clearing House Symposium entitled "Rationalizing the U.S. Anti-Money Laundering and Counter Terrorist Financing Regime: Are There More Effective Ways to Identify Criminals and Terrorists With Less Collateral Damage To Trade, Development and Other Goals?" on April 18, 2016 in Washington, D.C.

Juan C. Zarate is chairman and senior counselor for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance and is the chairman and co-founder of the Financial Integrity Network. **Chip Poncy** is a senior advisor for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance and is the president and co-founder of the Financial Integrity Network.

There have been herculean efforts to make the system work. Even with such dedication, the current AML/CFT system is not working effectively or systemically. It is inefficient in how it attempts to prevent financial crimes and ineffective in protecting the financial system from the flow of illicit financing. But this is not the time to abandon the principles embodied in this system. Quite the opposite – this is a moment of opportunity to design a new system that does more to protect the international financial system and reduce the costs and inefficiencies of the current model.

This memo explains why the current AML/CFT regime as designed and implemented is outdated and lays out a vision for a new AML/CFT approach – driven by new technologies and structural innovations – that is better designed to protect the integrity of the financial system.

Protecting the Integrity of the Financial System

The evolved goal of the AML/CFT regime is to protect the integrity of the financial system in a way that furthers key national security objectives, with a demand that financial institutions (especially major global banks) guard the gates of the global financial system. What was designed as a regime to help law enforcement "follow the money" has expanded to include a preventative web of sanctions and regulations used to deny rogue actors access to commercial and financial facilities. This evolution has placed enormous stress on the financial community to meet the expanding definitions of financial crime, complexities of sanctions regimes, and the heightened expectations of compliance.

The costs have been high. Billions of dollars of fines have been collectively levied against banks for failure to comply with legal requirements, and billions more have been invested in compliance systems, personnel, and remediation to meet increasing global AML/CFT standards and expectations. The stakes for financial security are even higher. Amid the increased scrutiny, illicit funds – from state and non-state actors – continue to flow. Criminal networks, rogue regimes, and terrorist groups continue to gain access to capital; they use the dark corners of the financial system, old and new methodologies, and developing technologies to circumvent or overwhelm the best of controls.

Estimates suggest that well over a trillion dollars of illicit financing are raised and moved globally every year, fueling everything from arms and human trafficking to environmental crimes and kleptocracy. These illicit flows also affect development and sustainable economic growth. In 2015, developing economies lost over a trillion dollars to illicit finance activities.[2] Successful efforts to prevent illicit financing, uncover criminal networks, or trace rogue capital seem difficult and sporadic at best. Even with increased vigilance and more reporting of suspicious activity, the volume of illicit financing continues to present systemic challenges to AML/CFT regimes around the world.

Recent events have reinforced the idea that the system is not working as intended. The Panama Papers leak exposed the purposeful opacity in corporate formation and the placement and layering of money and transactions that can facilitate all forms of financial crime and the evasion of sanctions. The continued fines and prosecutions of banks for failing to meet sanctions and AML obligations underscore the fact that compliance culture and practices have not met policy expectations. And global corruption investigations – such as the 1MDB scandal in Malaysia – reveal the corrosive force of unbridled power and money, and continued exploitation of the world's seemingly most well-regulated banks.

The policy and regulatory communities are already grappling with the question of whether the system is effective. In 2014, the Financial Action Task Force (FATF) launched a new round of assessments to test whether jurisdictions'

2. The World Bank Group, "The World Bank Group's Response to Illicit Financial Flows: A Stocktaking," March 22, 2016. (http://documents.worldbank.org/curated/en/502341468179035132/pdf/104568-BR-SecM2016-0112-IDASecM2016-0071-IFC-SecM2016-00423-MIGA-SecM2016-0044-Box394878B-PUBLIC-disclosed-4-5-16.pdf)

systems are effective, as opposed to simply in place on paper. Regulators and policymakers are considering how best to judge and balance financial transparency policies, exclusion of suspect activity, and inclusion of vulnerable communities/sectors. The private sector is grappling with its compliance obligations and whether its investments are worthwhile and sustainable.

The AML/CFT System is Flawed

Current AML/CFT efforts are systemically ineffective because of both incomplete implementation and outdated design.

There has not been a full commitment globally to the current model of compliance and transparency. Efforts have been hindered by the absence of a culture of compliance and a failure by financial and commercial actors to appreciate the heightened global expectations of financial integrity. The current system has also failed to regulate and shine a light on all vulnerable sectors of the global economy. A lack of resources and expertise within government authorities has led to weak enforcement, with a heavy reliance on the United States to police the system. Some of this ineffectiveness can be explained by a failure to effectively adopt, apply, supervise, and enforce appropriate risk-based models. The growing demands and risks to the financial sector have also engendered a defensive mindset that is less about risk management and more about risk avoidance.

It is legitimate to argue that the current system has never been fully or properly implemented. This ineffectiveness, however, is not just about a lack of understanding, commitment, or enforcement. The design of the AML/CFT system is outdated, and there are inherent limitations in the design of the current paradigm.

Structural Design Challenges

As designed, the current system is intended to support law enforcement in the investigation and prosecution of financial criminal cases, not as a way to defend the entire financial system from abuse. Traditionally, law enforcement agencies viewed the financial system as a means to discover and obtain information on criminals.[3] The Bank Secrecy Act (BSA), the foundation of today's AML/CFT system, was created in 1970 to assist law enforcement agencies in "following the money." The Suspicious Activity Reporting system that requires regulated entities to file suspicious activity reports (SARs) on dubious customers and transactions remains a tool for law enforcement to build cases.

As a result, AML/CFT reporting requirements and obligations are built on a "one-to-one" model, where each institution typically reports to an authority (usually a financial intelligence unit) about singular customers and transactions. The stove-piping of information is intended to protect customer data and reporting to law enforcement for the purpose of investigations. This model does not create a dynamic flow of information between authorities and institutions within the private sector, or across borders. In short, there is no facility for real-time responses, dynamic feedback, or collective learning.

There is a creeping recognition by regulators and the financial community that there needs to be new AML/CFT models to deal with the pressures of managing compliance risk and more opportunities to do so in a cost-effective and sustainable way.

3. National Commission on Terrorist Attacks Upon the United States, "Chapter 4: Combating Terrorist Financing in the United States: The Role of Financial Institutions," *Monograph on Terrorist Financing*, accessed September 14, 2016. (http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Ch4.pdf)

Thus, each institution's visibility into illicit activity ends with its touch points with customers and transactions, and most authorities are not seeing systemic vulnerabilities across institutions on a real-time basis. Within institutions, information sharing between business lines and compliance teams happens on a customer-by-customer basis. It is difficult for both the public and private sectors to monitor and respond to systemic vulnerabilities without specific focus and enormous resources. And if the private sector proactively uncovers vulnerabilities, such focus is often met with additional regulatory scrutiny.

All attempts and structures to facilitate broader information sharing – such as through the Egmont Group of Financial Intelligence Units (FIUs) or Section 314(b) of the USA Patriot Act, which permits financial institutions to share information under certain criteria – are intended to break these barriers. The major global banks have tried to shape this with the development of their own FIUs. Regulated institutions have developed "Super SARs" to report networks of concern within their platforms or businesses. Despite these innovations, the current design is still a transactional-based model that is not geared toward systemic defense.

Policy Challenges

The increased use and blending of sanctions and the AML/CFT system to exclude financial rogues and to maximize financial transparency has created a series of escalating risks and policy challenges for the private sector. Regulators and policymakers continue to demand that the financial community understand and manage its risk – often demanding that institutions know and monitor not only their customers but also their customers' customers, transactions, and suppliers. Authorities are deputizing these same companies, ramping up requests for banks to register, collect information, and report suspicious activity.[4] This also includes discovering and even predicting where illicit actors are operating before authorities list related individuals or entities.

These escalating risks are compounded by the costs of catching up with financial transparency expectations now codified with the new customer due diligence (CDD) rule in the U.S. and the heightened global importance of understanding ultimate beneficial ownership.

The need to address these systemic vulnerabilities has contributed to decisions by institutions to bluntly de-risk customers, business lines, and jurisdictions. The justifiable concern with these risks has often overshadowed the need to focus on threats that institutions face from illicit financing networks that exploit their businesses.

The reality is that sophisticated organized crime groups, terrorists, and rogue states continue to find ways to leverage the financial system to increase their wealth and global reach. Mexican drug cartels have used banks to move billions of dollars; North Korea is a criminal state that has evaded sanctions through front companies and its trade with China; and terrorist groups such as Hezbollah have developed global trafficking networks that laundered funds through banks and money service businesses (MSBs). The very elements of globalization that facilitate trade and commerce also allow illicit actors to leverage that system for profit.

Institutions faced with expanding policy expectations are left with no choice but to de-risk or expend enormous resources to invest in the tools and personnel needed for compliance. This puts a premium on quantitative metrics used to show seriousness of purpose and effectiveness, such as the filing of SARs and the number of compliance officers hired. However, these metrics often fail to produce qualitative differences in risk management. These factors have not necessarily led to a more effective AML/CFT system.

4. Aruna Viswanatha, "More Than Ever, Banks Play the Role of Government Law-Enforcement Agents," *The Wall Street Journal*, July 28, 2016. (http://www.wsj.com/articles/more-than-ever-banks-play-the-role-of-government-law-enforcement-agents-1467883802)

Technical Challenges

The mission of countering illicit finance also faces a massive technical challenge. The 1980s analog model that developed to understand, screen, and monitor customers and transactions has not kept pace with the amount, speed, and fluidity of data available in the 21st century. The new digital and big data economy is transforming all businesses. In the past, most regulated institutions segmented their data systems to meet business needs, not to optimize compliance management. That is changing, but financial crime risk management depends on the platforms, data, and analytics upon which compliance relies.

The risk of making the wrong compliance decision has put a premium on creating more sophisticated escalation processes and tweaking the algorithms and models used to flag suspicious behavior. The refinement of these systems is limited, however, by unstructured or missing data as well as lack of connectivity between internal and external data sources. Even with attempts at technical patches and greater automation in the public and private sectors, the SAR process and network analysis often relies on manual reviews. The result is an almost impossible mission of fighting 21st century financial crimes using 20th century technologies.

Whether due to a failure to commit to a culture of compliance or adopt a true risk-based model, or the failings of design and technical challenges posed by an outdated system, the current approach is not geared toward meeting the demands of defending the global financial and commercial systems from abuse by illicit actors. A new design could help leapfrog over those deficiencies.

Reimagining the AML/CFT System

Fortunately, we now have the opportunity to reimagine the current system and make it more effective. There is a creeping recognition that there needs to be a new cost-effective and sustainable model for managing compliance risk.

New technologies are blazing the trail for a novel approach. Capabilities that allow organizations to collect, share, analyze, and protect mass amounts of data and transactions in real time, establish more reliable customer and transaction identification, and apply more sophisticated and automated analytic tools are the cornerstone for a new model. From 2013 to 2020, the digital universe will grow by a factor of 10 – from 4.4 trillion gigabytes of data to 44 trillion,[5] which means it more than doubles every two years. Such a monumental shift is fueled by the rapid increase in "virtualized datacenters, seamless public and private cloud computing, and new storage management technologies," according to IDC.[6] In the realm of regulatory technology, new tools allow for more collaborative sharing of information in smarter and more effective ways.

There are a variety of new technologies, data aggregation mechanisms, platforms, and pilot programs that could help shape and build confidence in a new AML/CFT system.

It is now possible to consider what the design of a new system might look like. Like a common utility, this system would involve participating institutions to automatically share bulk customer and transaction information. Automated analytics would be applied against transactions to screen sanctioned and suspect parties and identify patterns of concern on a real-time basis. Red flags would be provided to participating institutions,

5. "The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things," *International Data Corporation*, April 2014. (http://www.emc.com/leadership/digital-universe/2014iview/index.htm)
6. Ibid.

relevant authorities, and FIUs. Information provided could be anonymized to protect customer privacy, while transactions and reports to relevant parties would be provided in real time. This model could be applied on different platforms and involve different actors, in some cases with government, including FIUs, at the center, and in others a private sector actor or consortium acting as the trusted clearinghouse. There are seven core principles that are critical to this new design:

1. Prevention and Risk-Based Paradigm: There must be a recognition – in law, practice, and design – that the AML/CFT system needs to move from a reactive model to a preventative, risk-based model. The intent is not simply to respond to criminal activity but to prevent illicit actors from accessing the financial system. There also needs to be a commitment to true risk management and allowance for financial firms to engage in risk-taking, especially when trying to meet the goal of financial inclusion.

2. Sector-Wide Protection: The system needs to be constructed to protect financial and commercial sectors broadly and collectively. This means that key sectors – such as the global banking community, the insurance sector, investment firms, and particular businesses – would be viewed and treated as a whole to prevent them from being abused. This would allow for high-risk sectors to manage their risk collectively and provide necessary assurances to the marketplace.

3. More Data and More Sharing: Higher-quality data and greater information sharing would be essential for this model, using big data capabilities, biometrics and identity verification, and network and behavioral analysis. This would include automatic sharing of cross-border wire data, customer transaction information, and suspicious activity information within organizations and sectors and across borders. This would also include real-time feedback loops and continuous learning and analysis for use by the participants, and would take advantage of any new technologies, such as blockchain, or other digital tools.

4. Automation and Analytics as Drivers: Leveraging more powerful analytics and automation to discover and even predict where suspicious illicit behavior or vulnerabilities may lie will be essential to any new system. This would require a common understanding of how such analytics would be used to screen customers, monitor transactions, and reveal illicit activity – and an acceptance that there would be shared risk in the calibration of relevant algorithms and typologies. This would also take advantage of the evolution and use of artificial intelligence, where machines can recognize patterns of behavior over time.

5. Enhanced Privacy and Protection: Trust in any new model is essential for it to work. Any new model must reinforce the security of individuals' information and the protection of privacy and civil liberties. Technologies can be applied to mask and protect sensitive customer data – for privacy and proprietary reasons – while allowing for effective network analysis and anomaly detection. Any data aggregation would need to be paired with the best cybersecurity practices and systems.

6. Risk Sharing and Management: This new model requires there to be shared risk among like actors in specific sectors, along with more robust, shared risk management between the public and private sectors and between governments. Parties must be comfortable sharing more information and managing risk together, and governments must be willing to help inform and manage risk along with the private sector. This model could extend to collaboration among correspondent banks. With more information comes more responsibility. All actors would need to allow for a model of shared financial crime and sanctions risk management.

7. Cost Sharing: Though the new model would not alleviate the need for each institution to invest and engage in baseline compliance risk management or for governments to create regulatory and enforcement capacity, it would

provide for a collective platform to analyze sector-wide risks. Over time, this would allow for the reliance on capabilities that are collectivized and automated. This could also provide a more sustainable cost model that can be shared among participants.

There are challenges to implementing any new model on a global or even jurisdictional basis. Existing legal strictures, bureaucracies and calcified cultures, regulatory expectations, sunk systemic costs and investments, lack of agreement on the common model, and risk of massive change all suggest this will not be easy. The good news is that innovations are already emerging, and the vision for a new AML/CFT paradigm is appearing in pieces in various new platforms, technologies, and pilot programs.

Emerging Elements of a New System

There are a variety of new technologies, data aggregation mechanisms, platforms, and pilot programs that could help shape and build confidence in this new system.

Innovative Technologies

With customer identification, the field of biometrics is rapidly evolving. Countries such as India are at the forefront of this area, with the biometrics market in India predicted to reach $3 billion by 2021.[7] Banks are beginning to introduce "touch ID" log-in capabilities for their customer accounts (for example, mobile banking apps).[8] In addition, biometric fusion – including iris scans and voice recognition – is providing banks with alternative ways of confirming a customer's identity.

New payment models and the financial technology market are transforming the way customers and transactions are accessing financial services. Alternative payment providers and systems are challenging banks' traditional dominance of the sector, and younger consumers and those outside of the traditional banking system are adopting a wider range of payment options.

The rise of digital ecosystems provides opportunities for innovation that could enhance financial efficiency and compliance. Financial institutions are beginning to embrace the underlying blockchain technology (which provides an open public ledger for transactions). Other banks are joining consortia such as R3 to collaborate on exploring and developing distributed ledger technologies that can be leveraged by the financial sector. Regulators in advanced economies are finding the balance between regulating new financial products and services and allowing for innovation.

The distributed ledger technology is being imagined as a secure way to record contracts, facilitate remittance payments, and revamp trade finance. It "offers the intriguing possibility of eliminating [banks as the] 'middle man' by filling three important roles – recording transactions, establishing identity, and establishing contracts – traditionally carried out by the financial services sector," as Bernard Marr wrote in *Forbes*.[9] Technology giants are moving toward

7. "Indian biometric market to be worth $3 billion by 2021," *Planet Biometrics*, July 6, 2016. (http://www.planetbiometrics.com/article-details/i/4695/desc/indian-biometric-market-to-be-worth-3-billion-by-2021/)
8. Linn Foster Freeman, "Banks embracing biometric technology," *Data Privacy + Security Insider*, June 30, 2016. (https://www.dataprivacyandsecurityinsider.com/2016/06/banks-embracing-biometric-technology/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29)
9. Bernard Marr, "How Blockchain Technology Could Change The World," *Forbes*, May 27, 2016. (http://www.forbes.com/sites/bernardmarr/2016/05/27/how-blockchain-technology-could-change-the-world/#34580db49e09)

promoting the technology, and in May 2016, Microsoft announced that it had joined the Chamber of Digital Commerce,[10] the world's largest trade association representing the digital asset and blockchain industry. The data captured and shared via blockchain allows for analysis well beyond the immediate transaction and allows targeted insights into global illicit financial streams.[11] With these new technologies deepening customer and transactional identification, the potential for the identification of suspicious patterns and networks increases exponentially.

Aggressive Information-Sharing Structures

Information-sharing platforms are emerging to optimize how parties are sharing information. These are beginning to open the possibility for more collaborative models of information sharing, including customer information.

In the United Kingdom, for example, the Joint Money Laundering Intelligence Taskforce (JMLIT) links government agencies, law enforcement bodies, and 25 major UK and international banks. JMLIT's approach is based on a model of "collaboration, collective ownership and prioritization" to combat high-end money laundering.[12] The approach has worked well. JMLIT members have developed cases, identified and closed banks accounts, obtained 50 new court orders, and made numerous arrests. As a result, the UK government now plans to move JMLIT to a more permanent footing and expand its membership.[13]

In the United States, there is movement toward more active models of information sharing under Section 314(b) of the USA Patriot Act. The Office of the Comptroller of the Currency, the Department of Justice, and the Treasury Department's Office of Terrorism and Financial Intelligence have all expressed their support for 314(b) communications.[14] Efforts by Standard Chartered Bank, Bank of America, and Wells Fargo to focus information-sharing efforts on combating human trafficking are good examples of this practice. Financial Crimes Enforcement Network (FinCEN) reports demonstrate a steady growth in the number of SARs explicitly referencing 314(b) communications from banks, broker-dealers, insurance companies, and financial services companies, among others.[15]

The cyber domain is also providing an arena and models for greater collaboration. Major U.S. banks have recently announced efforts to collaborate to protect against cyberattacks. Other platforms and alliances already demonstrate the success of dedicated real-time information sharing between the public and private sectors.

Countries and the financial industry are also beginning to collaborate and consolidate know-your-customer (KYC) databases and systems. India and France have established KYC platforms. In 2010, India's Credit Information Bureau (CIBIL) and several other industry associations launched CIBIL Mortgage Check, a nationwide tool for fraud control lauded by Business Standard as the country's "first centralized nationwide database of mortgage

10. "Microsoft joins blockchain-focused Chamber of Digital Commerce," *Microsoft*, May 4, 2016. (https://blogs.microsoft.com/firehose/2016/05/04/microsoft-joins-blockchain-focused-chamber-of-digital-commerce/#sm.001e9zdav1de7fc0v322b4nj8clog)
11. Kristofer Readling and Justin Schardin, "Why Blockchain Could Bolster Anti-Money Laundering Efforts," *Bipartisan Policy Center*, June 2, 2016. (http://bipartisanpolicy.org/blog/blockchain-anti-money-laundering/)
12. UK Joint Money Laundering Intelligence Taskforce, "Public-private information sharing partnerships to tackle money laundering in the finance sector: The UK Experience," accessed September 14, 2016. (http://thecommonwealth.org/sites/default/files/inline/4%20UK%20approach%20to%20public-private%20partnerships.pdf)
13. City of London Police, "New taskforce brings together law enforcement, Government and the financial sector to crack down on fraud," February 10, 2016. (https://www.cityoflondon.police.uk/news-and-appeals/Pages/New-taskfirce-brings-together-law-enforcement.aspx)
14. Denise Hutchings, "5 insightful FinCEN statements about Collaboration through 314(b)," *CUInsight*, September 22, 2015. (https://www.cuinsight.com/5-insightful-fincen-statements-about-collaboration-through-314b.html)
15. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "The SAR Activity Review: Trends, Tips & Issues," May 2013. (https://www.fincen.gov/sites/default/files/shared/sar_tti_23.pdf)

information that will help banks and financial institutions share and access mortgage information, exercise stronger due diligence, and reduce fraudulent transactions."[16] France operates a central database of bank accounts known as FICOBA (Fichier national des comptes bancaires et assimilés), which is managed by the French tax administration and holds more than 80 million account registrations.[17] Other countries, including the United Kingdom, have announced efforts to establish corporate registries to facilitate CDD requirements, which may provide another vehicle for analyzing bulk customer data.

In addition, the banking industry is working with organizations such as KYC.com to share customer information as a means to make adding customers more efficient, share costs, and avoid bank arbitrage by nefarious actors. This platform could prove helpful in allowing the banking sector to share more information and costs.

Real-time information-sharing mechanisms used in other contexts, such as fraud detection and prevention, may also provide helpful examples of how customer and transaction information can be shared and used efficiently by competitors to protect sectors against illicit activity.

Screening Platforms

Common screening systems and platforms present an intriguing opportunity to consolidate compliance risk management and to share the risk attendant to addressing illicit finance.

In Mexico, the central bank has established the Banco de México's Domestic USD Transfer System (SPID), an electronic domestic payment system designed for the settlement of interbank U.S. dollar payments between Mexican banks. Launched in 2016, SPID was developed in part to increase traceability and transparency of dollar-denominated transactions within the Mexican financial system, and it requires enhanced AML/CFT obligations of all participating banks through the central bank's role as operator. As SPID members, banks are specifically required to apply more stringent AML/CFT policies and reject transactions of which they do not approve on AML/CFT or fraud grounds.[18]

SPID has not yet become fully functional, and financial crime risks and questions remain, including how transparent the system will be, whether it could shield suspect dollar transactions from U.S. authorities, and how it responds to real risks to the Mexican system. Despite those questions, SPID provides an opportunity to think creatively about how a credible national authority might use the real-time collection, screening, and analysis of financial data and transactions to identify and respond to vulnerabilities and threats to the banking sector.

Such national centralization efforts are echoed by corresponding supranational developments, such as the consolidated transaction monitoring and analytic systems from the Society for Worldwide Interbank Financial Telecommunication (SWIFT). In late 2014, SWIFT launched its KYC Registry, a secure shared platform for financial

16. "CIBIL and TransUnion launch CIBIL Mortgage Check," *Business Standard* (India), September 2, 2010. (http://www.business-standard.com/article/companies/cibil-and-transunion-launch-cibil-mortgage-check-110090200169_1.html)
17. Markus Meinzer, "Bank account registries in selected countries: Lessons for registries of trusts and foundations and for improving automatic tax information exchange," *Tax Justice Network*, August 21, 2012. (http://www.taxjustice.net/cms/upload/pdf/BAR2012-TJN-Report.pdf)
18. "Domestic USD Transfer System (SPID)," *Banco de México*, March 2016. (http://www.banxico.org.mx/sistemas-de-pago/servicios/sistema-de-pagos-interbancarios-en-dolares-spid/%7B3DBBBDBD-055F-1289-0201-9C307BB9EA63%7D.pdf)

institutions to exchange and manage standardized KYC data, developed in collaboration with the industry.[19] To date, approximately 2,000 banks in 191 countries are using it as a cost-effective way to improve the efficiency of their operations, reduce cost, and mitigate risk.[20] SWIFT has also launched the Sanctions Screening service, which allows for real-time message screening for institutions, especially midsize institutions, against 30 sanctions lists.

These types of platforms and screening models could be expanded beyond sanctions screening to include the monitoring, analysis, and flagging of illicit financing. They could also be combined with models of centralized collection of transaction information in addition to enhanced KYC information sharing. Australia and Canada have developed noteworthy models to capture cross-border transfer information and opportunities for systemic analysis and information sharing among multiple stakeholders.

The Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian FIU, collects, analyzes, and disseminates financial intelligence data on cross-border currency transactions, suspicious transactions, and large currency transactions. AUSTRAC oversees the compliance of – and collects data from – more than 14,000 Australian businesses, including major banks, casinos, and single-operator businesses.[21] Canada is using a similar approach through its Financial Transactions and Reports Analysis Centre (FINTRAC). FINTRAC first required the reporting of cross-border electronic funds transfers (EFTs) made via SWIFT messages in 2002 and expanded the reporting requirement to cover all forms of international EFT regardless of the system used.[22]

The United States has long flirted with systemic reporting of cross-border wire transfer information. In September 2010, FinCEN proposed a regulatory requirement that would require certain banks and money transmitters to report transmittal orders associated with certain cross-border electronic transmittals of funds. Officials argued that "by establishing a centralized database, … an exceptional benefit to law enforcement and the modest cost to industry" could be leveraged.[23]

In 2015, FinCEN announced its intent to revisit its 2010 proposal to capture information on all bank cross-border wires and non-bank remittances of $1,000 or more.[24] FinCEN's renewed interest was sparked by the completion of the FinCEN IT Modernization Project, which now gives the bureau the systems and information technology platforms required to collect and analyze the large volume of cross-border electronic funds transfers. The U.S. government has not yet moved toward the capture of all cross-border wire information, but the technical possibilities may spur its eventual collection and analysis.

19. Society for Worldwide Interbank Financial Telecommunication, "The KYC Registry: Your source for Know Your Customer information," accessed September 14, 2016. (https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/the-kyc-registry)
20. Bryan Yurcan, "Banks Prove Willing to Band Together Under KYC Pressure," *American Banker*, January 14, 2016. (http://www.americanbanker.com/news/bank-technology/banks-prove-willing-to-band-together-under-kyc-pressure-1078835-1.html)
21. Australian Transaction Reports and Analysis Centre, "About AUSTRAC," accessed September 14, 2016. (http://www.austrac.gov.au/about-us/austrac)
22. U.S. Department of the Treasury, Financial Crimes Enforcement Network, "Appendix E – Cross-Border Funds Transfer Reporting in Canada and Australia," *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act*, October 2006. (https://www.fincen.gov/sites/default/files/shared/Appendix_E.pdf)
23. U.S. Department of the Treasury, Financial Crimes Enforcement Network, Press Release, "FinCEN Proposes Regulatory Requirement for Financial Institutions to Report Cross-Border Electronic Transmittals of Funds," September 27, 2010. (https://www.fincen.gov/sites/default/files/shared/20100927.pdf)
24. Brian Monroe, "With IT Modernization Finished, FinCEN Again Raising Cross-Border Funds Transmittal Initiative," *Association of Certified Financial Crime Specialists*, June 4, 2015. (http://www.acfcs.org/news/300828/With-IT-modernization-finished-FinCEN-again-raising-cross-border-funds-transmittal-initiative.htm)

An important step toward greater transparency and risk management is a new FinCEN reporting requirement, announced in May 2016, that requires financial institutions to identify and verify the identity of beneficial owners of legal entity customers, which would enhance the effectiveness of analyzing cross-border wire transfer information.

Safe Harbors and Experimentation

Regulators and policymakers need to allow for greater experimentation and be open to collectivized models of risk management, including between the government and the private sector. The UK's Financial Conduct Authority (FCA) has led these efforts, and announced in May 2015 the creation of a "regulatory sandbox," a safe space in which businesses can test innovative products, services, business models, and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question.[25] Participating firms will report on agreed-upon milestones during testing, and the FCA will then publish findings from sandbox testing to educate the industry on any findings and emerging best practices.

In the United States, a more permissive use of Section 314(b) to include involvement of technology companies may provide greater freedom to experiment with information-sharing platforms and mechanisms. The expansion of models such as the JMLIT would also assist in creating the trust and mechanisms necessary as platforms for a new model to emerge.

Globally, this requires a commitment to, and allowance for, more aggressive information sharing while still respecting privacy and civil liberties protections. Without this, enterprise-wide risk management and a more advanced model of sector-wide information sharing will be stunted.

For industry, this requires a commitment to innovation, with most major banks investing in innovation teams to account for technological advances and industry changes. This also means finding internal efficiencies and breaking down internal barriers for information sharing and risk management. For example, the blending of separate systems and platforms used for compliance, fraud, cybersecurity, and business intelligence may prove essential for protecting major global institutions against evolving vulnerabilities and risks. Shared systems and defenses may allow for greater efficiency and innovation. Finally, more aggressive information sharing by the private sector will require greater regulatory cooperation and deference to encourage experimental "sandboxes" to pilot such collective risk management and network analysis initiatives.

Conclusion

Despite unprecedented efforts, the current AML/CFT system is not working systematically, efficiently, or effectively, and it must be improved beyond short-term fixes to promote the security and integrity of the financial system. Such improvements should allow for the simplification of regulatory requirements while improving the effectiveness of controls. The solution is emerging, enabled by new technologies and the recognition that we need to establish a sustainable and shared compliance risk management system. We are on the brink of developing this new paradigm for protecting the integrity of the financial system and national security. We need to continue to experiment and design a new model with a clear road map and principles in mind. This is the path to an effective and sustainable AML/CFT system.

25. UK Financial Conduct Authority, "Regulatory sandbox," December 9, 2016. (https://www.fca.org.uk/firms/project-innovate-innovation-hub/regulatory-sandbox)

About the Authors

Juan C. Zarate is chairman and senior counselor for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance and is the chairman and co-founder of the Financial Integrity Network. Juan served as the Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism from 2005 to 2009 and was the first-ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes. Chip Poncy is a senior advisor for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance and is the president and co-founder of the Financial Integrity Network. From 2002 to 2013, he served as the inaugural director of the Office of Strategic Policy for Terrorist Financing and Financial Crimes and a senior advisor at the U.S. Department of the Treasury. Chip led the U.S. delegation to the Financial Action Task Force (FATF) from 2010-2013, co-chaired the policy working group of the FATF from 2007-2013, and managed U.S. participation on various G7, G8 and G20 illicit finance experts groups from 2008-2013.