THE QUARTERLY JOURNAL OF *THE CLEARING HOUSE* Q3 2016, VOLUME 4, ISSUE 3

BANKING PERSPECTIVES

DESIGNING A MORE EFFECTIVE AML/CFT SYSTEM

STRENGTHENING THE RISK-BASED APPROACH

HAS THE U.K. FOUND THE ANSWER TO AML INFORMATION SHARING?

TECH'S ROLE IN IMPROVING THE AML SYSTEM

AML REFORM: A SAFE HARBOR PROPOSAL

Fixing AML

The Clearing House®
At the Center of Banking Since 1853®

The more people understand how their money works, the more confident they'll feel about their financial decisions. That's why we created Better Money Habits in partnership with Khan Academy — an independent, nonprofit organization with the mission of providing a free, world-class education for anyone, anywhere. Better Money Habits is a one-of-a-kind online approach to financial education that's customizable and answers tough financial questions in practical ways.

BetterMoneyHabits.com

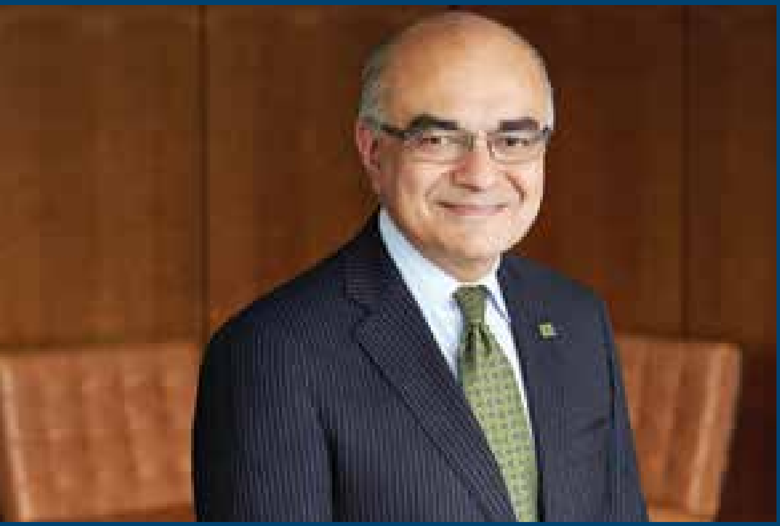
Better Money Habits®

Powered by Bank of America in partnership with KHANACADEMY

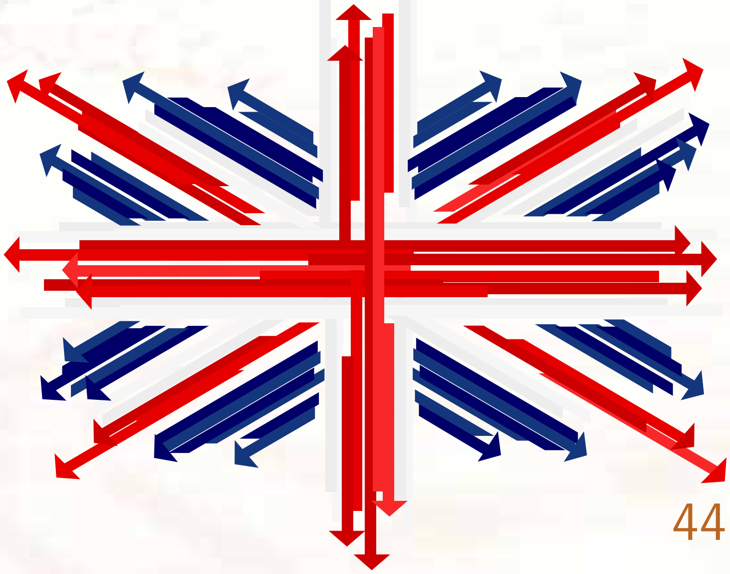
BANKING PERSPECTIVES

THE QUARTERLY JOURNAL OF *THE CLEARING HOUSE* Q3 2016, VOLUME 4, ISSUE 3

UPFRONT



FEATURED ARTICLES



DEPARTMENTS

The Clearing House®
At the Center of Banking Since 1853®

EDITOR Greg MacSweeney

DESIGN & PRODUCTION Big Yellow Taxi, Inc.

Banking Perspectives is the quarterly journal of The Clearing House. Its aim is to inform financial industry leaders and the policymaking community on developments in bank policy and payments. The journal is a forum for thought-leadership from banking industry executives, regulators, academics, policy experts, industry observers, and others.

Established in 1853, The Clearing House is the oldest banking association and payments company in the United States. It is owned by the world's largest commercial banks, which collectively hold more than half of all U.S. deposits and which employ over one million people in the United States and more than two million people worldwide. The Clearing House Association L.L.C. is a nonpartisan advocacy organization that represents the interests of its owner banks by developing and promoting policies to support a safe, sound, and competitive banking system that serves customers and communities. Its affiliate, The Clearing House Payments Company L.L.C., which is regulated as a systemically important financial market utility, owns and operates payments technology infrastructure that provides safe and efficient payment, clearing, and settlement services to financial institutions, and leads innovation and thought leadership activities for the next generation of payments. It clears almost $2 trillion each day, representing nearly half of all automated clearing house, funds transfer, and check-image payments made in the U.S.

The Clearing House

1114 Avenue of the Americas
New York, NY 10036
212.615.9250

1001 Pennsylvania Avenue, NW
Washington, DC 20004
202.649.4600

Contributors

Sharon Cohen Levin

Sharon Cohen Levin, a partner at WilmerHale, is an authority on anti-money laundering, the Bank Secrecy Act, economic sanctions, and asset forfeiture. Levin served for 19 years as Chief of the Money Laundering and Asset Forfeiture Unit in the U.S. Attorney's Office for the Southern District of New York. Levin has worked closely throughout her career with state and federal banking regulators, the U.S. Treasury Department's Office of Foreign Asset Control, the Financial Crimes Enforcement Network, and the Department of Justice. Levin has a J.D. from the University of San Diego School of Law and a B.A. from Tulane University.

Sabreen Dogar

Sabreen Dogar is a financial crime compliance manager at HSBC. Before joining HSBC, she worked as an intelligence analyst for the U.S. Department of Homeland Security, with a focus on transnational criminal organizations.

Thomas Donegan

Thomas Donegan, a partner in Shearman & Sterling's global Financial Institutions Advisory & Financial Regulatory Group, advises financial institutions, including banks, exchanges, clearinghouses, and settlement systems on legal and regulatory issues.

Donegan advised on the implementation and impact of the EU/U.K. regulatory reforms arising out of the recent financial crisis and how local initiatives fit into the global regulatory architecture including on EMIR, MiFID II, capital, recovery and resolution, governance, ring-fencing, the EU single market program, anti-money laundering issues, and shadow banking reforms.

Tom Keatinge

Tom Keatinge is Director of the Centre for Financial Crime & Security Studies at the Royal United Services Institute (RUSI), a London-based defense and security think tank. Keatinge's published research covers topics including the role of finance in defeating al-Shabaab; the role of financial intelligence in identifying and disrupting foreign terrorist fighters; and a number of articles considering ISIS financing. Prior to joining RUSI in 2014, Tom was an investment banker for 20 years at J.P. Morgan.

Clay Lowery

Clay Lowery is VP at Rock Creek Global Advisors, an international economic policy advisory firm, where he focuses on international financial regulation, sovereign debt, exchange rates, and investment policy. He is also a visiting fellow at the Center for Global Development and a senior adviser at the Center for Strategic and International Studies. Lowery served as the assistant secretary for international affairs at the US Treasury Department from 2005 to 2009 and chaired the Committee on Foreign Investment in the United States. He was the point person on U.S. policy toward sovereign wealth funds; served as the Finance Deputy to the G20, G7, International Monetary Fund, and the Financial Stability Forum; and was appointed by the President at various times to be the U.S. representative to the boards of the World Bank, African Development Bank, European Bank for Reconstruction and Development, and Inter-American Development Bank.

Chip Poncy

Chip Poncy is the President and Co-Founder of the Financial Integrity Network and a Senior Advisor for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance. From 2002 to 2013, Poncy served as the inaugural Director of the Office of Strategic Policy for Terrorist Financing and Financial Crimes (OSP) and a Senior Advisor at the U.S. Department of the Treasury. As the Director of OSP from 2006 to 2013, he led an office of strategic policy advisers in creating policies and initiatives to combat the full spectrum of illicit finance, including money laundering, terrorist financing, WMD proliferation financing, and kleptocracy flows.

Poncy graduated with honors from Harvard University (B.A. in government) and The Johns Hopkins School of Advanced International Studies (M.A. in international relations), and holds a J.D. from Georgetown University.

Vijaya Ramachandran

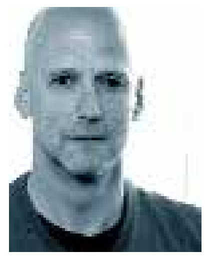
Vijaya Ramachandran is a senior fellow at the Center for Global Development (CGD). She works on private sector development, anti-money laundering, illicit financial flows, food security, humanitarian assistance, and development interventions in fragile states. Prior to joining CGD, she served on the faculty at Georgetown University and also worked in the Africa Private Sector Group of the World Bank and in the Executive Office of the Secretary-General of the United Nations. Ramachandran earned her Ph.D. in business economics from Harvard University.

Barnabas Reynolds

Barnabas Reynolds is head of the global Financial Institutions Advisory & Financial Regulatory Group and is Global Co-Head of Financial Institutions at Shearman & Sterling. He advises financial firms on their businesses in the London and European markets. He focuses on financial institution law and regulation and legal risk management, both national and cross-border. From 2010 to 2014, he served as an elected member of the firm's Policy Committee.

Reynolds advises on the implementation and impact of the EU/U.K. regulatory reforms arising out of the recent financial crisis and how local initiatives fit into the global regulatory architecture, including on the impact and implementation of MiFID II, regulatory capital, recovery and resolution, ring-fencing, the EU single market program, Ukraine/Russia sanctions, anti-money laundering issues, and shadow banking reforms.

Gary Shiffman, Ph.D.



Gary Shiffman, Ph.D., is an expert in the economics of national security, and he focuses on using social science and network and data analysis to protect the world from illicit actors. Shiffman's aim is to make it difficult for criminals and terrorists to accomplish their goals.

In addition to his work as the founder and CEO of Giant Oak, Shiffman has been a professor at Georgetown University since 2002. His past professional experiences have positioned him as an expert in the unique intersection between the social sciences, big data, business, and national security concerns. These include service as Managing Director of the Chertoff Group, Senior Vice President and General Manager of the Risk Management Solutions business unit at L-3 Communications, and Chief of Staff at U.S. Customs and Border Protection.

Shiffman is a decorated U.S. Navy Gulf War veteran. He earned his Ph.D. (economics) from George Mason Univ., his M.A. (security studies) from Georgetown Univ., and his B.A. (psychology) from the Univ. of Colorado.

Bob Werner

Bob Werner is a former federal prosecutor and was the head of both the U.S. Financial Crimes Enforcement Network and the U.S. Office of Foreign Assets Control. During

his career in the private sector, he has headed financial crime compliance functions at several global financial institutions. He is currently the Global Head of Financial Crime Compliance at HSBC, and he is based in London.

Juan C. Zarate

Juan C. Zarate is the Chairman and Co-Founder of the Financial Integrity Network, the Chairman and Senior Counselor for the Foundation for Defense of Democracies' Center on Sanctions and Illicit Finance, and the Senior National Security Analyst for NBC News and MSNBC. He is also a Visiting Lecturer of Law at the Harvard Law School, a Senior Adviser at the Center for Strategic and International Studies, and a Senior Fellow to the Combating Terrorism Center at West Point.

Zarate served as the Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism from 2005 to 2009, and was responsible for developing and implementing the U.S. Government's counterterrorism strategy and policies related to transnational security threats. He was the first-ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes, where he led domestic and international efforts to attack terrorist financing, the innovative use of Treasury's national security-related powers, and the hunt for Saddam Hussein's assets.

He is a magna cum laude graduate of Harvard College, a cum laude graduate of Harvard Law School, and a former Rotary International Fellow at the Universidad de Salamanca, Spain. ■

FOR THE RECORD

Time for an AML Reboot

BY GREG BAER

Imagine an army where officers are not evaluated based on how they or their units behave in battle, or how well they lead their troops. Rather, the officers are considered for promotion based on audits of the punctuality of their expense reports, and whether supplies are accounted for and documented with 100% accuracy. Any reporting or documentation errors result in confinement to base, extensive retraining, and reduction in pay.

The auditors also track unit casualties, with any casualty resulting in demerit, demotion or court martial for the responsible officers. The auditors do not have sufficient seniority or clearance to be briefed on the battles that have occurred, or read any after-action reports. Thus, their audits reflect only the losses suffered by the unit itself, not the casualties it inflicted upon the enemy.

GREG BAER is President of The Clearing House Association and Executive Vice President and General Counsel of The Clearing House Payments Company. He oversees the legal, compliance, and litigation functions for the organization's payments business and leads the strategic agenda and operations of the Association. Prior to joining TCH, Baer was Managing Director and Head of Regulatory Policy at JPMorgan Chase.

What sort of an army would this system produce? Certainly, one hesitant to take risk. While a patriotic desire to defeat the enemy would remain strong, officers would know that outside-the-box thinking would result in audit lapses, and eventually end their careers. Promotion would come for those who adhered to the rules, and excelled at paperwork. This army inevitably would end up being led by a George McClellan, not a Ulysses S. Grant. Morale among the troops would plunge.

Welcome to the U.S. anti-money laundering /counter-terrorism financing regime, circa 2016. It is a system in which banks have been deputized to act as quasi law-enforcement agencies. Their AML compliance staffs collectively represent a force somewhere between the size of the ATF and the FBI, spending billions of dollars each year to investigate and report crime. However, in talking to senior executives at banks large and small, I have never heard a single one complain about how much money they spend. Rather, they complain about how much of that money is wasted. And that waste derives from a series of perverse incentives embedded in an archaic system.

From a public policy perspective, any rational approach to AML/CFT law enforcement would be risk-based, devoting the great majority of resources to detecting the most dangerous financial crimes and illicit activity. However, as described by Bob Werner of HSBC, the former head of the U.S. Financial Crimes Enforcement Network (FinCEN), we have seen a move by large banks away from risk-based approaches, because banks are not rewarded for successfully uncovering money laundering or providing valuable service to the law enforcement, defense or intelligence communities. Such acts generally are unknown to the bank examiner evaluating their performance or the Justice Department official deciding on a fine for some unrelated transgression. Rather, the key obligation of banks under the current AML regime is a requirement to file suspicious activity reports (SARs), which originated in 1992 as a way for banks to provide leads to law enforcement. In the current regulatory and enforcement climate, compliance officers at banks have powerful incentives to file numerous SARs, because those defensive SAR filings protect them in the event that one of the companies or individuals involved ultimately commits some type of crime. But that defensive approach greatly increases the ratio of noise to signal – or, in an analogy one frequently hears, simply adds more hay to the search for the AML/CFT needle.

Furthermore, banks receive almost no meaningful feedback on how those SARs are used, or which ones proved useful to law enforcement. In the 1970s, when few reports were filed, those that did generally received serious law enforcement attention, and feedback was less. Now, with banks employing tens of thousands of people and using computer monitoring to flag potentially suspicious activity, hundreds of thousands of SARs are being filed every year. Feedback therefore would be extremely useful – particularly for the work of people like Gary Shiffman, the founder of a data analytics company, who uses big data technology to analyze data from across the industry to find criminal patterns.

Meanwhile, the pressure on banks to maintain perfect AML/CFT procedures is unrelenting. Procedural lapses, even those of no consequence, can endanger the careers of those involved. Because examiner criticism endangers the ability of the bank to expand, pressure for 100% accuracy is intense. One senior AML executive recently said, "I can't remember the last time I tried to catch a bad guy; I spend all my time filing reports with regulators." Worse yet, several others have reported that their own efforts to construct novel approaches to detecting illegal behavior have resulted in examiner criticism – because such innovative approaches lacked sufficient documentation, and therefore were not auditable.

The sources of this self-defeating set of perverse incentives are not difficult to discover: the unpopularity of banks; the politicization of agency enforcement actions; a movement at the Justice Department away from a "justice-based" model to a "leveraged-based" enforcement model;[1] and Congressional hearings where both banks and their examiners are excoriated for real or perceived shortcomings.

Indeed, the plight of bank examiners is worth considering. From a political perspective, they can only do wrong. They are excluded when the bank they examine is working real cases with law enforcement, national security or intelligence community officials. But if something goes wrong – if a corrupt official or organization turns out to be a client of the bank they examine – then they are held to account. Thus, from an examiner and banking agency perspective, the best possible outcome is for the banks they supervise to "de-risk" – that is, retreat from high-risk jurisdictions abroad and high-risk businesses domestically. They have no reason to internalize the business loss suffered by the bank from de-risking, nor the loss to national security when the intelligence community loses the ability to monitor overseas jurisdictions as illicit finance moves to shadow markets, nor the human suffering in countries cut off from correspondent banking, money remittances, or other access points to the global financial system. Contrast this state of affairs with the cooperative, more innovative approach in the United Kingdom, described herein by Tom Keatinge, Director of the Centre for Financial Crime and Security Studies at the Royal United Services Institute.

Perverse incentives extend to rule writing as well. Writing a clear and public AML/CFT standard means accepting great responsibility. It means defining what is an acceptable approach to preventing money laundering and terrorist financing, and what is unacceptable. If a bank engages in conduct defined as acceptable and wrongdoing nonetheless occurs, then the regulator can be held accountable. A clear remedy here would be the establishment of safe harbors for banks that demonstrate they have thorough AML/CFT procedures – recommended here by Sharon Cohen Levin, former Chief of the Money Laundering a Asset Forfeiture Section of the U.S. Attorney's office for the Southern District of New York. But creating a safe harbor requires the government to give up the ability to punish if something goes wrong, and suffer second guessing for it. On the other hand, abjuring clear rules and using enforcement action or private threats thereof (the latter protected from public scrutiny and awareness

as "confidential supervisory information") poses no such risks.

Think these issues through, and it is easy to understand the spectacle of Secretary of State John Kerry's recent visit to the United Kingdom. The reason for his visit was frustration that, notwithstanding an agreement to lift sanctions on Iran, companies seeking to do business with Iran were having difficulty obtaining banking services. The stated goal of his visit was to "make clear that legitimate business, which is clear under the definition of the agreement, is available to banks as long as they do their normal due diligence and know who they're dealing with. They're not going to be held to some undefined and inappropriate standard." The reaction of the banking community could be boiled down to "easy for you to say." *The Wall Street Journal* put it more eloquently: "Some banks say that they have made up their minds on not doing business with Iran, in part because they have agreements in place with U.S. agencies that may take a different view than the official government stance on Iran." In other words, Secretary Kerry need not have traveled to London: a trip down the street to the Justice Department and the bank regulatory agencies would have been more effective.

Or consider FIFA. Various FIFA officials have been indicted, or in some cases pled guilty to receiving bribes to award the World Cup to certain countries. The investigation was a tribute to the Justice Department and FBI, and a relief to soccer fans everywhere. But while public attention has moved on, the investigation of banks that processed the payments continues. No one would be surprised if the banks end up paying more in legal fees and fines than any of the bribe takers or bribe payers. Nor should they be surprised, of course, if U.S. banks decide to "de-risk" such organizations going forward.

As Clay Lowery and Vijaya Ramachandran demonstrate graphically herein, AML/CFT-related fines on U.S. banks have increased exponentially over the past five years, and continue to do so. There can be no doubt that the billions of dollars in fines, coupled with supervisory restrictions on banks perceived as having subpar programs, have caused banks of all sizes to devote vastly more resources to AML/CFT processes. The ultimate, and really only important questions, are: have these resources, and the sanctions and regulatory regime that produced them, made our country safer and more prosperous, or less? And would a very different regime produce far better results?

That is a difficult question, with a complicated answer. While it is good to keep bad actors out of the financial system as a sanctions matter, does it benefit national security to keep bad actors in the system, where they can be monitored by regulated banks with sophisticated techniques? Or is it better to push illicit actors out to foreign banks or hawalas, where law enforcement has little line of sight and a much harder time tracking money movement? Is any law enforcement or counter-terrorism gain worth causing poverty in countries that harbor terrorists by using the blunt force of pressuring U.S. banks to "de-risk" those countries by ending correspondent relationships? Are the vast quasi-law enforcement resources of the banks better deployed marching in lock step, under rigid policies and procedures set by regulators, or by using idiosyncratic guerrilla tactics, emphasizing innovation? Should banks be filing more SARs under a low standard for what constitutes suspicious activity, or instead be filing fewer SARS under a higher standard focused on plausible evidence of serious wrongdoing?

Furthermore, it is somewhat odd that there is a continuing, heated political debate about U.S. trade policy, but that the considerable effects of AML/CFT rules are not part of that debate. Rightly or wrongly, those rules are serving as major impediments to trade finance, reducing exports and imports, and causing a retreat by U.S. banks and corporations behind our borders.

Unfortunately, in the public debate, there thus far has been little acknowledgment of these important tradeoffs. Fines and personal liability for compliance officers continue to increase; and banks are required to cast a wider net in investigating their customers, and their customers' customers.

Fortunately, a remarkable group of foreign policy, development and technology experts – including the contributors to this issue – has been focusing on all these issues. Their goal is not to save banks money or embarrassment. Their goal is do what is best for our country. We at the Clearing House will do everything we can to assist them in their work, because the banks we represent – and more particularly the tens of thousands of individuals at those banks doing this work, many of whom are former military, intelligence or law enforcement officials – are desperate to innovate and investigate. They want to catch the bad guys too. ■

---

1 In a recent speech, former Deputy Attorney General David Ogden has described how the Department of Justice "has moved away from traditional notions of prosecutorial discretion, founded in self-discipline about the facts and the law... and moved towards a greater willingness to use leverage to negotiate maximum fines and penalties." https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/News/Documents/2016-06-09-Keynote-Remarks-Delivered-at-US-Chamber-of-Commerce-Institute-for-Legal-Reform-and-National-Association-of-Criminal-Defense-Lawyers-Symposium.pdf

MY PERSPECTIVE

Unintended Consequences of Tighter Liquidity Requirements

BY BILL NELSON, THE CLEARING HOUSE

Janet Yellen, chair of the Federal Reserve Board and the Federal Open Market Committee (FOMC), is worried that r* has been falling. We are, too – as you should be. A low r* poses a big problem. And bank regulations might be making the problem worse.

What, you ask, is r* (pronounced "r star")? Among economists, it is known as the equilibrium (or neutral) real federal funds rate. I realize that probably doesn't help, so let's break it down.

1. In the United States, the FOMC (the Federal Reserve System's monetary policy-setting body) conducts monetary policy by setting a target for the overnight federal funds rate, one of the interest rates banks charge each other for overnight credit.

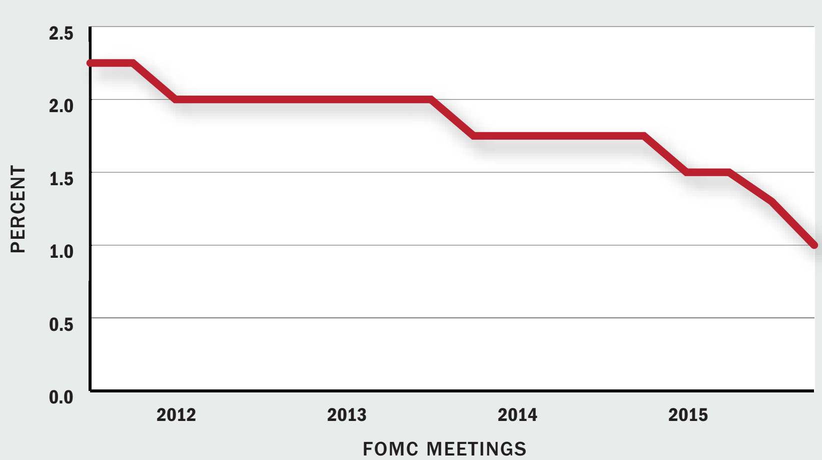
2. A real interest rate is the nominal (stated) interest rate minus inflation, and it's the real interest rate that links monetary policy to economic activity.

3. Monetary policy works primarily by raising the real interest rate to slow the economy and reduce inflation and lowering the real interest rate to speed up the economy and increase inflation.

4. The equilibrium real federal funds rate (r*) is the rate above which the FOMC slows the economy and below which the FOMC stimulates the economy. It's the Goldilocks interest rate.[1]

Each quarter, as part of the economic projections it releases with the minutes of its meetings, the FOMC provides its estimate of r* that is expected to prevail in the longer run. As you can see in Figure 1, its estimate of r* has been falling steadily since it started providing the projections at the beginning of 2012, and recently it's been dropping even faster.

FIGURE 1: MEDIAN FOMC FORECAST OF LONGER-RUN REAL FEDERAL FUNDS RATE



WHY IS A LOW R* A BAD THING?

A low r* is a bad thing for two reasons, both tied to the fact that nominal interest rates can't fall below zero.[2] First, the lower that r* is, the less stimulus to economic activity the FOMC can provide. As pointed out earlier, the stimulus provided by monetary policy is determined by the amount that the real interest rate falls below r*. If inflation is running at the FOMC's target of 2%, the FOMC can't reduce the real interest rate below -2% (the minimum nominal rate of 0 minus the inflation rate of 2%). If r* is 2%, then the FOMC can deliver, at most, 4 percentage points of stimulus by setting the federal funds rate at 0. But if r* is, say, 1%, the FOMC can only deliver, at most, 3 percentage points of stimulus.

But that's not the worst of it. Over the longer run, a lower r* increases the likelihood that the United States will once again find itself trapped at the zero lower bound. Assuming that the FOMC can keep inflation near its 2% target, nominal interest rates (real interest rates plus inflation) will tend to trend around r* plus 2%. Given the FOMC's current

estimate of r* at 1%, interest rates will normally be about 3%. But during past recessions, the FOMC has, on average, lowered the federal funds rate by 4.5 percentage points.[3] A similar decline would leave the federal funds rate at the zero lower bound, requiring the FOMC to resort to nontraditional measures such as buying longer-term securities in order to pull down longer-term interest rates.

Even worse, those nontraditional measures tend to be less effective, raising the possibility that inflation will fall in the recession despite the easing of policy.[4] As inflation falls, monetary policy becomes even less stimulative, because the real federal funds rate rises; inflation could then fall further, and a deflationary spiral could develop.

In short, a low r* is very bad and potentially dangerous.

WHY IS R* FALLING?

A number of reasons have been given for why r* is so low, and why it keeps falling. For one, the headwinds holding back economic growth after the financial crisis tend to push down r*; however, those headwinds appear to have dissipated. In the news conference following the June 2016 FOMC meeting, Janet Yellen also pointed to more persistent factors such as slow productivity growth and the aging of the population.[5]

HOW MIGHT TIGHTER LIQUIDITY REGULATIONS LOWER R*?

Another possible reason why r* has been falling is the tightening of liquidity regulations that has occurred over recent years. That possibility was first identified last year by a working group of central bankers, convened by the Bank for International Settlements (BIS) to assess the cumulative impact that the package of new bank regulations known as Basel III is having monetary policy.[6] They noted that tighter liquidity regulations make very short-term financial instruments more valuable than longer-term instruments, which

> **The NSFR would do little** to nothing to help fortify or measure bank liquidity, but it would contribute to a **further decline in r*.**

will pull down short-term interest rates relative to intermediate- and longer-term rates:

> In jurisdictions where the central bank primarily influences the overnight rate, but longer-term interest rates are more relevant for economic activity, *the central bank will thus need to target a somewhat lower level of interest rates to achieve the same economic outcome* [emphasis added].

The United States is in the situation that the working group identified: The central bank primarily influences the overnight rate, and longer-term rates are more relevant for economic conditions. So according to the BIS working group, because of the tightening of liquidity regulations, the FOMC will have to target a lower real federal funds rate to get the same economic outcome. In other words, tighter liquidity regulations will lower r*.

IT GETS WORSE

The added demand for short-term liquid assets from tighter liquidity requirements that could be pushing down r* also boosts the "money premium," the extra amount that investors will pay for a money-like asset. An elevated money premium can also have serious consequences. When the money premium is high, the interest rates on money-like instruments are lower than other instruments. Private financial intermediaries take advantage of this money premium to issue certain types of collateralized short-term debt, such as asset-backed commercial paper, or engage in repo transactions. This "private money creation" was a big part of the growth in the shadow banking sector in the years preceding the financial crisis, where seemingly safe maturity and

WILLIAM (BILL) NELSON is Executive Managing Director, Chief Economist, and Head of Research, The Clearing House Association, and Chief Economist of The Clearing House Payments Company. Nelson contributes to and oversees research and analysis to support the advocacy of the Association on behalf of the owner banks. Prior to joining The Clearing House in 2016, Nelson was a deputy director of the Division of Monetary Affairs at the Federal Reserve Board.

liquidity transformation led to the run-like behavior in financial markets observed during the crisis.

In a recently released TCH research note, we provide evidence that the money premium is currently elevated.[7] Indeed, that evidence is part of why we think tighter liquidity regulations may be one of the factors lowering r*. If the money premium is elevated, it could be providing incentives that could lead to continued and accelerating growth of the shadow banking system in the future.[8]

> **As the Federal Reserve's** balance sheet and financial conditions normalize, the NSFR will bind increasingly tightly on banks, **boosting the demand** for liquid assets even further.

POSSIBLE POLICY RESPONSES

A tightening of liquidity regulation and supervision is a critical and appropriate part of the U.S. authorities' response to the financial crisis. Important components of that tightening have been the establishment of the liquidity coverage ratio (LCR) requirement (which requires banks to have 30 days' worth of emergency liquidity at all times) as well as the creation of the annual Comprehensive Liquidity Analysis and Review, a horizontal examination of the liquidity of the largest banks. However, as discussed in a recent TCH research note, there are already reasons to conclude that the next and final component of the tightening of liquidity requirements, the net stable funding ratio requirement (NSFR), which is out for comment, is neither helpful nor necessary.[9] The NSFR is like the LCR, only it's designed to ensure that a bank has sufficient liquidity over a one-year horizon. As discussed in that note, as the Federal Reserve's balance sheet and financial conditions normalize, the NSFR will bind increasingly tightly on banks, boosting the demand for liquid assets even further. In that case, the NSFR requirement will add further to the upward pressure on the money-premium and the downshift in r*.

As discussed in Stein et al. (2015), there are a number of ways that the government could respond to the squeeze on money-like instruments. The Treasury could fund itself increasingly with bills rather than notes or bonds, or the Fed could acquire less-liquid assets and fund its purchases by creating more reserve balances. But the first rule when you find yourself in a hole is to stop digging. The simplest policy response would be to refrain from adopting the NSFR requirement. The NSFR would do little to nothing to help fortify or measure bank liquidity, but it would contribute to a further decline in r*. ■

ENDNOTES

1 R* is often confused with, but is not the same as, the interest rate called for by a monetary policy rule (such as the Taylor rule). Monetary policy rules prescribe tighter or looser policy in reaction to the economic situation; that is, they call for appropriate deviations from r*. One way to define r* is as the interest rate called for in a monetary policy rule when inflation is at target and the economy is at capacity.

2 Interest rates have recently fallen below zero in some countries, but they can't fall much further.

3 Haldane, Andrew. "Stuck," speech given to Open University, London. June 30, 2015. http://www.bankofengland.co.uk/publications/Pages/speeches/2015/828.aspx

4 Engen, Eric, Thomas Laubach, David Reifschneider. "The Macroeconomic Effects of the Federal Reserve's Unconventional Monetary Policies." Finance and Economics Discussion Series. Federal Reserve Board. January 15, 2015.

5 "Transcript of Chair Yellen's Press Conference." Federal Reserve. June 15, 2016. https://www.federalreserve.gov/mediacenter/files/FOMCpresconf20160615.pdf

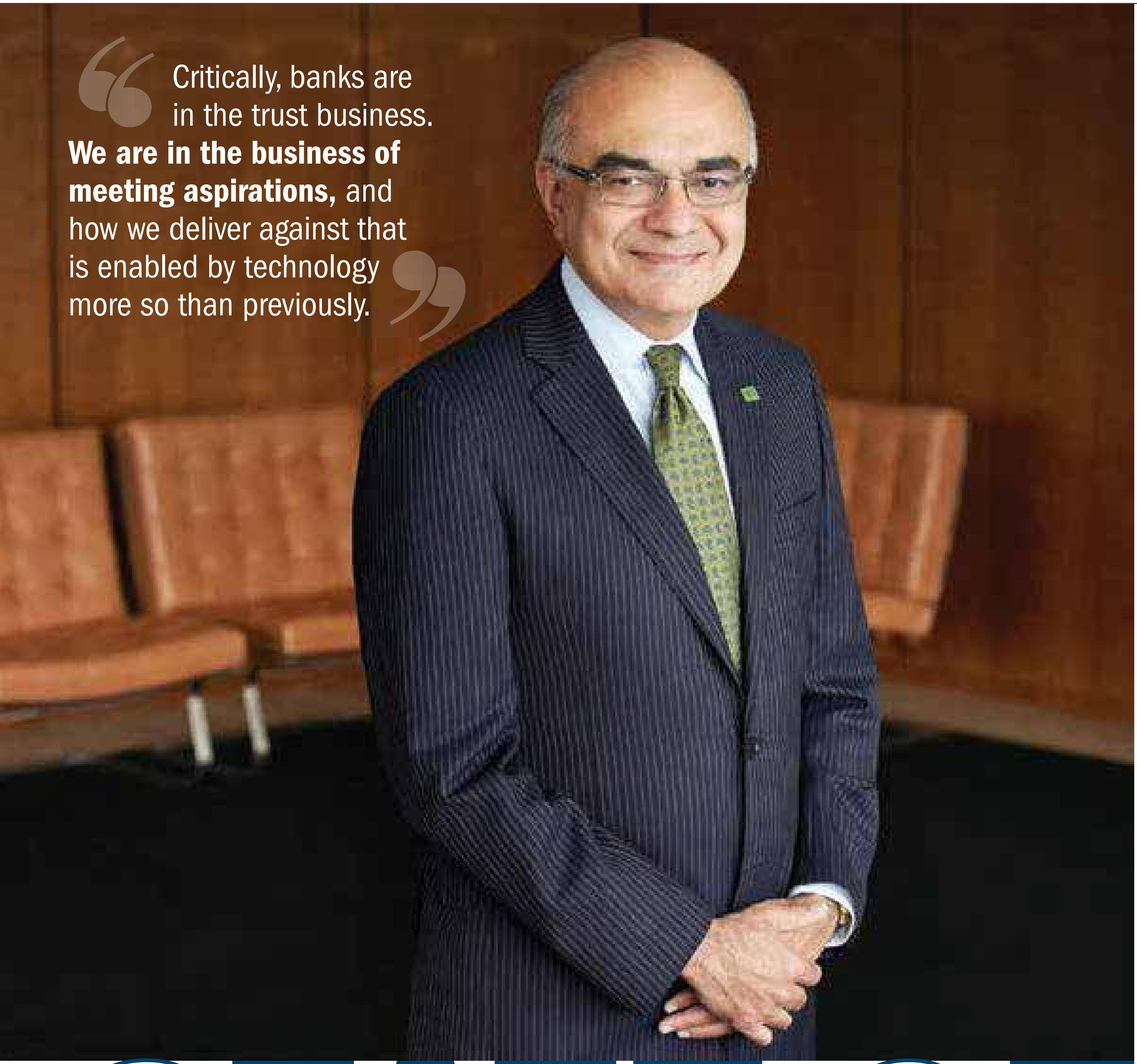
6 "Regulatory Change and Monetary Policy." CGFS Papers No. 54. Committee on the Global Financial System and the Markets Committee. May 2015.

7 "Liquidity Regulations, R*, and the Money Premium." TCH, August 2016.

8 Tarullo, Daniel. "Opening Remarks at the Center for American Progress and Americans for Financial Reform Conference." July 12, 2016.

9 "The Net Stable Funding Ratio: Neither Necessary nor Harmless." TCH, July 2016. https://www.theclearinghouse.org/~/media/TCH/Documents/20160705_TCH_NSFR_Note.pdf

"Critically, banks are in the trust business. **We are in the business of meeting aspirations,** and how we deliver against that is enabled by technology more so than previously."



STATE OF

Bharat Masrani, Group President and Chief Executive Officer of TD Bank Group, discusses how the industry has changed over the years, TD's approach to innovation, and evolving customer expectations with **Jim Aramanda**, CEO of The Clearing House.

JIM ARAMANDA, TCH: *You've had an extensive career in banking during your 29 years at TD. How has the role of an executive changed? What is required to run a multinational bank today as opposed to when you started in the industry?*

BHARAT MASRANI, TD BANK: First of all, Jim, as for my 29 years at TD Bank, I can't get a job anywhere else! What can I tell you? But to answer your question, great companies, and by extension great leaders, don't stay great by staying the same. It's an old saying, and I think it really applies to our industry. I firmly believe that companies that endure figure out ways to adapt to the environment they find themselves in rather than hoping and praying that the situation goes back to the good old days. The pace of change that we are experiencing now is probably the fastest that I've experienced in my 29 years in banking.

We are seeing technological and demographic changes. We are seeing customer expectations evolve quite dramatically. We're seeing regulatory changes that are coming fast and furious, and great companies – and, again, great leaders – find a way to adapt. The ones who are able to adapt faster than others have a distinct advantage.

Ultimately, the competitive structure of banking has changed. If you look at the old days in Banking 101, we used to talk about barriers to entry. Those barriers still exist, but they're very different today than they were 20 years ago. Companies need to recognize that, adapt, and transform to be successful on an ongoing basis.

ARAMANDA: *You also were the Vice Chair and Chief Risk Officer of TD Bank Group for a few years (2003–2006). How did your tenure at CRO help you in subsequent positions?*

MASRANI: I've been very fortunate to have been able to build a varied career that has spanned almost 30 years, all within TD. During this time, I've touched nearly every aspect of TD's operations across three continents – including in the U.K., India, and the U.S.

One of the most pivotal moments during my time as CRO was making the decision to exit the structured financial products business. This was before the financial crisis, and we, [former TD CEO] Ed Clark and I, were criticized at the time for it. We struggled with the business model. On the one hand, it made the bank a lot of money, and the Street loved it. On the other hand, few people truly understood it. We felt it was the right thing to exit the business. We were working to build a franchise dealer, and complex securities didn't make sense.

That experience – and indeed all of my career experience at TD – has helped me to stay focused on doing the "right

BANKING

thing," which is doing what is in the best interest of our customers, colleagues, and shareholders.

ARAMANDA: *As you mentioned, changing customer expectations have transformed banking. Today, banks have to meet customers where they are. Customers often no longer come to the bank. Technology is a great enabler and has helped to drive this transformation. How is technology helping meet and exceed customer expectations?*

MASRANI: As you say, technology is an enabler, and sometimes that is lost on bankers. It's not technology for technology's sake. Technology enables us to make a difference and help us meet our customers' aspirations, such as buying a home, or saving for their kids' education, or for retirement. That's the business that banks are in. Critically, banks are in the trust business. We are in the business of meeting aspirations, and how we deliver against that is enabled by technology more so than previously. If banks today can deliver what customers are looking for and preserve the relationships and the trust, then I believe banks can continue to thrive.

Technology is now a huge factor and customers expect us to adapt, but it's equally important to make sure that, as we take advantage of new technologies, we continually look for ways to improve processes and make it easier for our colleagues to get their jobs done and for our customers to bank seamlessly with us. Our goal is clear – to deliver legendary customer experiences in the online and mobile space, just as we have in our stores and contact centers.

ARAMANDA: *While we're on the topic of technology, where is TD focusing its mobile efforts now, and can you speak to the work being done at TD's innovation centers?*

MASRANI: TD has more than 24 million customers, not counting TD Ameritrade. Many of these are in retail and commercial banking. Out of those 24 million customers, nearly 11 million of those would be online and mobile customers.

Customers will connect with us, transact with us, get advice from us, buy products from us if and how they wish, rather than us forcing them to a particular channel or product. We want to have an experience at the front end that is seamless whether our customers come through mobile or through one of our stores.

So, how do we do that? Mobile and digital play an important role. That is one way technology enables us to provide such an experience. We are finding a way to provide those services and products where the touch points are seamless and, frankly, opaque to the customer.

We have been able to create that initial engagement by coming up with innovations like TD MySpend, which is an app that allows customers to easily track their spending habits. We launched it in April, and we have 500,000 customers using TD MySpend in Canada. Not only is it a mobile app, but it's totally integrated with what we are doing in the bank. Now, how did we do that?

First, we recognize opportunities in the marketplace, saying there's a need for this. This is what our customers want. This is what our customers are telling us. Then, how do we build the technology to fulfill those needs with all the complications that come from a bank? It requires attracting special talent.

This brings us to the innovation centers we've set up. We have a few of them. We're also an investor in Communitech [Kitchener, ON]. We are the only bank that is involved in this technology partnership.

We have taken an approach that involves partnering with a lot of startups, and innovation companies, as well as working on our own stuff. We're investors in certain innovation hubs, and we've created our own technology centers as well. This multifaceted approach allows us to play in this arena where close to 11 million customers are now engaged with us on a regular basis to experience what we are providing in the online and the mobile space.

ARAMANDA: *How do you see your ability to attract the technology talent that you are bringing into TD will help the bank stay ahead of the many new technology-oriented entrants that are trying to get into the banking space?*

MASRANI: We're collaborating with startups and big tech to look at emerging technologies and create more intuitive and personalized customer experiences. We talked about our innovation centers. We also recently announced that we were the first Canadian bank to join Plug and Play Tech Center in Silicon Valley, which is the largest global technology accelerator, as part of its FinTech program.

That not only allows us to innovate and experiment, but we are able to attract talent. So, these are kids, effectively very young – which tells you how old I am – who want to do these amazing things. We are able to not only leverage the talents for this particular, specific app they might be working on, but then they become part of our bank. I was so happy to hear from some of those folks who've joined us who said, "Oh my God, I never knew a bank to be as exciting as TD is in this space." Take TD MySpend. That in itself has meant more interest of folks wanting to join TD, who could not imagine a bank would come up with it.

As a bank, we have advantages that are immense. Other new entrants don't have these advantages, and we ought to recognize those advantages. For instance, I remember when ATMs came out. They said that this was the death of banking. The branches will disappear. What are banks going to do? Well, we're still here. Then, online banking comes along in the mid-'90s and people said, banks are dead. Bury them. Today, online banking is dominated by big banks. I think the same thing is playing out again. While I'm not underestimating some of the threats we have, banks will adapt, and we will succeed in this world as well.

Sometimes, whenever we're going through these phases, we bankers, because all of us who want to recognize the opportunities as well as the risk, sometimes tend to overreact. We say, "Oh my God. This is such a big event that is going to dramatically transform banking. We're not going to recognize the bank tomorrow." My own experience in life has been that generally these things work out more predictably than people realize.

ARAMANDA: *Payments is an area where there are many innovative things happening right now. And as you know, TCH and its banks are building a real-time payments system for the U.S. How does this play out? How do you see banks evolving in the payments space?*

MASRANI: We are prepared to compete, win, and grow in this space. More Canadians do their digital banking with us than any other financial institution in the country. We recently announced Apple Pay for our Canadian customers, a service we already offer to our U.S. customers. We have a strong suite of mobile payment options that include our TD app, Samsung Pay in the U.S., and our participation in UGO Wallet in Canada. We opened the TD-Cisco Lab in Toronto and are partnering with them on enhancing the banking experience. We're also part of a global group of financial institutions looking to leverage blockchain technology for secure data management.

> **We're collaborating** with startups and big tech to look at emerging technologies and create more **intuitive and personalized** customer **experiences**.

We are making investments in areas that we might not have made a few years ago, like digitization and mobile payments, and finding new ways to meet customer needs.

ARAMANDA: *Moving on, you helped establish TD's retail presence in the U.S. market when TD acquired Banknorth. TD Bank in the U.S. is about a third of your profits. Where do you expect most of the growth to come from in the future?*

MASRANI: Just to give you some context, TD in the U.S. has been there for more than 100 years because we've had presence in New York in the securities business and the wholesale banking business. But, in the pure retail banking space, we entered only in 2005 with a 51% acquisition of Banknorth, which at the time had $30 billion in assets.

Then, after that, we started some of the acquisitions and what you see today, which is over 1,200 locations from Maine to Florida. Every state on the Eastern Seaboard

except for one [Georgia], close to 9 million customers. We have almost 26,000 talented, dedicated TD bankers who are there to serve their customers day in and day out.

We have a fantastic business in Canada, as you know, Jim. We are 161 years old, and it's just a fantastic position. That being said, when we made the decision to enter the United States, we took the view that yes, we have a huge amount of growth opportunities still left in Canada, and we continue to do that because there are a lot of products where we don't think we have our natural market share.

Notwithstanding that, at some point, Canada is not large enough to sustain that growth for the decades to come, and hence our entry into the United States, which is 10 times Canada's size. When we entered, the banking space was relatively fragmented, and there were opportunities we thought we could create.

I firmly believe it's still true that the U.S. will provide good growth potential over the long term for us, because of just the pure population dynamic, the competitive structure, and the market dynamics.

ARAMANDA: *I would expect that some of the decent-sized banks in the U.S. will consolidate over the next few years. Do you see acquisitions as part of your growth strategy?*

MASRANI: The good thing, Jim, is that we do have the size, scale, profile, and brand to compete with the very best in the U.S. That doesn't mean that we're not open to further expanding by acquisition. We've already done acquisitions through this phase.

During the financial crisis, TD was one of the few banks that was financially very strong. In fact, that was a time when we were still Aaa-rated. We were able to take advantage of this position and acquire banks from the FDIC. We've shown that notwithstanding our current, more than sufficient scale in the U.S., if the right opportunity were to present itself, we would certainly look at it seriously.

Then, given our balance sheet in the U.S., we could arguably be one of the most liquid banks because we have a loan-to-deposit ratio of around 50%. So, we have lots of room to grow both organically and through acquisitions. We've been doing credit card transactions with partners, etc., so we're quite open to that type of acquisition as well.

Our appetite for acquisitions is certainly there, but what has changed for us is that we don't have to do a deal just to create scale. The deal would have to make sense strategically, financially, and offer timing that suits us.

ARAMANDA: *Acquisitions involve new books of business, customers, assets, and often many branches. The future of the branch in banking is always an interesting topic. Do you see changes in the branch in the role that branches will serve?*

MASRANI: The short answer is yes. Let me give you some background. When I was running's TD's U.S. business, we had one model, and it was 5,200 square feet, this many teller stations, this is where the ATM goes, etc., etc.

Today, we have seven or eight different models in the U.S., plus different models in Canada. The role of the store or branch is evolving. What we used to do a few years ago in branches, those types of transactions are no longer relevant for our customers in those locations. They'd rather engage with us on their mobile phone or online.

The types of engagement we're having with our customers in our physical locations are already changing, and we are adapting to that. Take for example one of our newer stores in New York City, at 86th and Lexington. It's above a subway station so there are lots of commuters. We have ATMs and iPads for our customers' everyday banking. If they have a more complex need, like applying for a loan, we can connect them to experts at our contact center via video conferencing. And we post the subway schedule on our plasma screens so they can keep on time.

My view is that, yes, there is a role for a branch or a store. It's a very important role, but it is evolving as we evolve the branch to match our customers' needs.

ARAMANDA: *Let's discuss banking regulation. Since the crisis, banks are holding much more higher-quality and*

quantity of capital and liquidity. Research we have done at TCH has found that these higher standards, although they're making our banks safer and sounder, are also having a potentially negative impact on economic activity as well and pushing certain activities into the shadow banking sector.

How have higher capital and liquidity levels changed your business model? Has there been a negative impact on long-term economic growth as a result?

MASRANI: I'd say look at the capital levels and liquidity requirements on banks just before the crisis. With what we have learned, that obviously wasn't enough.

There were many grossly undercapitalized banks, and there were lots of banks that didn't have enough liquidity. While one could argue there are a lot of reasons why the financial crisis happened, I don't think many people can stand there and say there was zero contribution because of that particular dynamic.

I come from the view that reform on capital and liquidity was absolutely necessary given what we had experienced through the crisis. As usual, when you get into that situation, sometimes it's hard to get to the exact number or level that might be appropriate given the circumstances. Sometimes the pendulum goes a little further. Over time, it settles down where it ought to be. Whether the numbers we have now or the levels we have now are too much or not enough, time will tell as to what an optimal level is.

Capital levels should have some relationship with the risk and the balance sheet we run. If you look at TD's mix of businesses, our types of businesses, the type of risks that we manage, and the markets in which we operate, from our perspective we're very comfortable.

Having said that, does that have implications on the economy? I'm sure it does, because banks play a very important role. However, having economic growth for the sake of economic growth is not good if it's fueled by debt. We know how that movie will end, because we've seen it so many times before. So, healthy economic growth where we have healthy banks that are able to withstand the cycles that we have all experienced is a good thing.

Now, we'll see how these rules work out over time. I'm sure there will be tweaks that everybody will understand that need to be made, and we will get to the right number. But given the type of crisis we went through, it will probably take longer than what we've been used to in previous cycles.

ARAMANDA: *With your experience in Canada and in the United States, can you compare the relationships banks have with their respective regulators?*

MASRANI: There are a number of differences in the regulatory regimes in Canada and the U.S. One is that the Canadian system has been more principles-based whereas the U.S. tends to be more rules-based. Another is that in Canada there are simply fewer regulators, particularly at the federal level, while in the U.S. there are numerous regulators with different Congressional mandates.

With respect to how we approach regulatory relations, our view is that we are generally on the same side. We try to understand what our regulators are trying to achieve and then work hard to find the most efficient solution. We believe it is critically important for us as a bank, and for the industry, to have open and transparent relationships with our regulators, and we do.

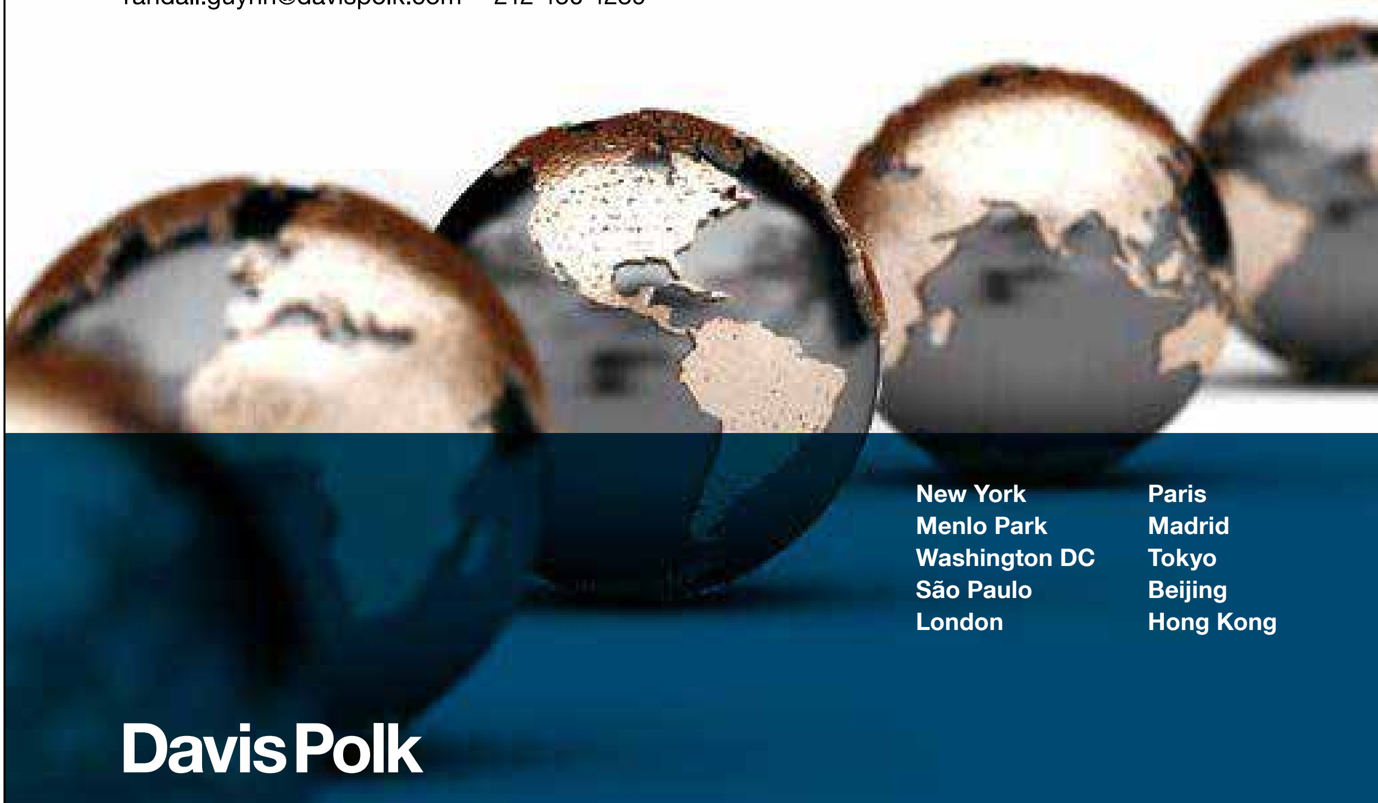
> **Let's make sure** if the activity is bank-like, it deserves bank-like regulation. Let's make sure that we look at it now and come up with **rules and regulations** that make sense for such activities. Obviously, while most people I talk to have a hard time disagreeing with the rationale behind this, **how to do it is more complicated.**

Our financial regulatory clients rely on the exceptional, collaborative service we deliver. Their success is our focus.

Davis Polk's market-leading Financial Institutions Group represents many of the most important U.S. and non-U.S. banks, broker-dealers, insurance companies, trading markets and investment managers. Our lawyers are at the forefront of advising financial institutions on how Dodd-Frank Act and bank capital requirements impact their businesses.

For more about our financial regulatory services, please visit davispolk.com or contact:

Randall D. Guynn
Partner and Head of the Financial Institutions Group
randall.guynn@davispolk.com ■ 212 450 4239



davispolk.com

ARAMANDA: *Can you talk about the relationship with the regulators? How has the regulatory action, or inaction in some cases, affected growth? How do you work to build relationships with the regulators and our elected officials?*

MASRANI: I think all of us are trying to do the right thing for our industry, for our country, and we all are on the same side of the road. I firmly believe that. But, when we have the type of downturn we had and the huge reform bill that ensued, which fundamentally changed the regulatory landscape in the country, then you are going to have stresses that'll take time to sort out.

The biggest change that would be very helpful is, where necessary, to remove any ambiguity. We are into year six of Dodd-Frank reforms, and we're still working on certain types of rules that may make sense. As much clarity as we can have is better for the industry, and better for the regulatory agencies as well.

Certain things are just going to take longer, but it reminds me when SOX 404 came into being. There were a few years where it was so difficult for companies to manage and comply with all the requirements. I think the regulators also were learning. Today, if you were to ask companies how they're doing on their SOX 404, it's part of business as usual. My expectation is that once we get through this cycle there will be sufficient clarity on all the rules that are yet to be promulgated. Once they've been out there and tested, I think we will get into more business as usual.

ARAMANDA: *Switching gears, you've called for a regulatory environment that ensures the safety of customer information and the integrity of our financial system. How have regulators responded to the industry's call for a level playing field as it competes with the FinTech companies?*

MASRANI: I'd say firstly that I think competition is great. It makes all of us better. It is better for our customers and for our shareholders because it makes the incumbents more nimble and stronger.

But having said that, as I mentioned earlier, we are in the trust business. We don't make cars. We don't make computers. We're in the business of making sure that people's savings and their aspirations to buy homes are met in an appropriate manner. That is a big responsibility.

It's not just about our shareholders, but it's also about our customers and how we're engaging in the communities in which we live and operate, and all those things become as important. As you know, in our business if our customers and other stakeholders lose confidence, then it's game over, such as the integrity of the data we hold on our customers. Their monies are safe and sound with us and aren't pilfered away by fraudsters. I do worry that as new players come into the banking space, that sometimes those activities that need to be regulated are not. I don't think that bodes well for our industry.

I'm urging the industry not to wait for an event. Let's make sure if the activity is bank-like, it deserves bank-like regulation. Let's make sure that we look at it now and come up with rules and regulations that make sense for such activities. Obviously, while most people I talk to have a hard time disagreeing with the rationale behind this, how to do it is more complicated.

You see the headlines about some of the newer players who've come into the industry. With a slight hiccup, and before you know it, there could be a confidence issue. That's already playing out to a smaller extent and we've seen some service interruptions, security and solvency issues, but once something relatively large happens, unfortunately what'll happen is it will impact even the regulated banks. Let's mitigate that in advance rather than waiting for it to happen.

ARAMANDA: *Do you have any final comments?*

MASRANI: I'd say overall, I feel privileged to be a banker. Banking is a noble profession. Sometimes it has been put in question because of various events that have taken place, but I feel that we play a special role in people's lives, and that is a privilege for me and my fellow bankers. I know all of them think the same way, and everybody wants to make sure that we have a thriving industry because a thriving banking industry is critical to a thriving economy. ■

EY
Building a better working world
Is security the price to pay for innovation?
EY's global financial services team can help you transform and improve your cyber security capabilities.
ey.com/banking #BetterQuestions
The better the question. The better the answer. The better the world works.
© 2016 EYGM Limited. All Rights Reserved. ED0717

THERE IS GROWING RECOGNITION THAT THE EXISTING AML/CFT REGIME ISN'T WORKING AS INTENDED. NOW IS THE TIME TO RETHINK AND REBUILD A SYSTEM TO MEET TODAY'S GROWING DEMANDS.

DESIGNING A NEW AML SYSTEM

BY JUAN C. ZARATE AND CHIP PONCY
FINANCIAL INTEGRITY NETWORK AND
CENTER ON SANCTIONS AND ILLICIT FINANCE

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. 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.[1]

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's 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 can't 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.

There have been herculean efforts to make the system work. Even with such dedication, the current AML/CFT system isn't working effectively or systemically. It's inefficient in how it attempts to prevent financial crimes and ineffective in protecting the financial system from the flow of illicit financing. But this isn't 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 article 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 isn't 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 haven't 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' 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 and 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.

Thus, each institution's visibility into illicit activity ends with its touch points with customers and transactions, and most authorities aren't 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's 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 (FUIs) 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 haven't necessarily led to a more effective AML/CFT system.

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, which means it more than doubles every two years.[5] 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.

It's 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, 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 won't 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.

> "Regulators and policymakers need to allow for **greater experimentation** and be open to collectivized models of **risk management.**"

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 promoting the technology, and in May 2016, Microsoft announced that it had joined the Chamber of Digital Commerce, the world's largest trade association representing the digital asset and blockchain industry.[10] 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.

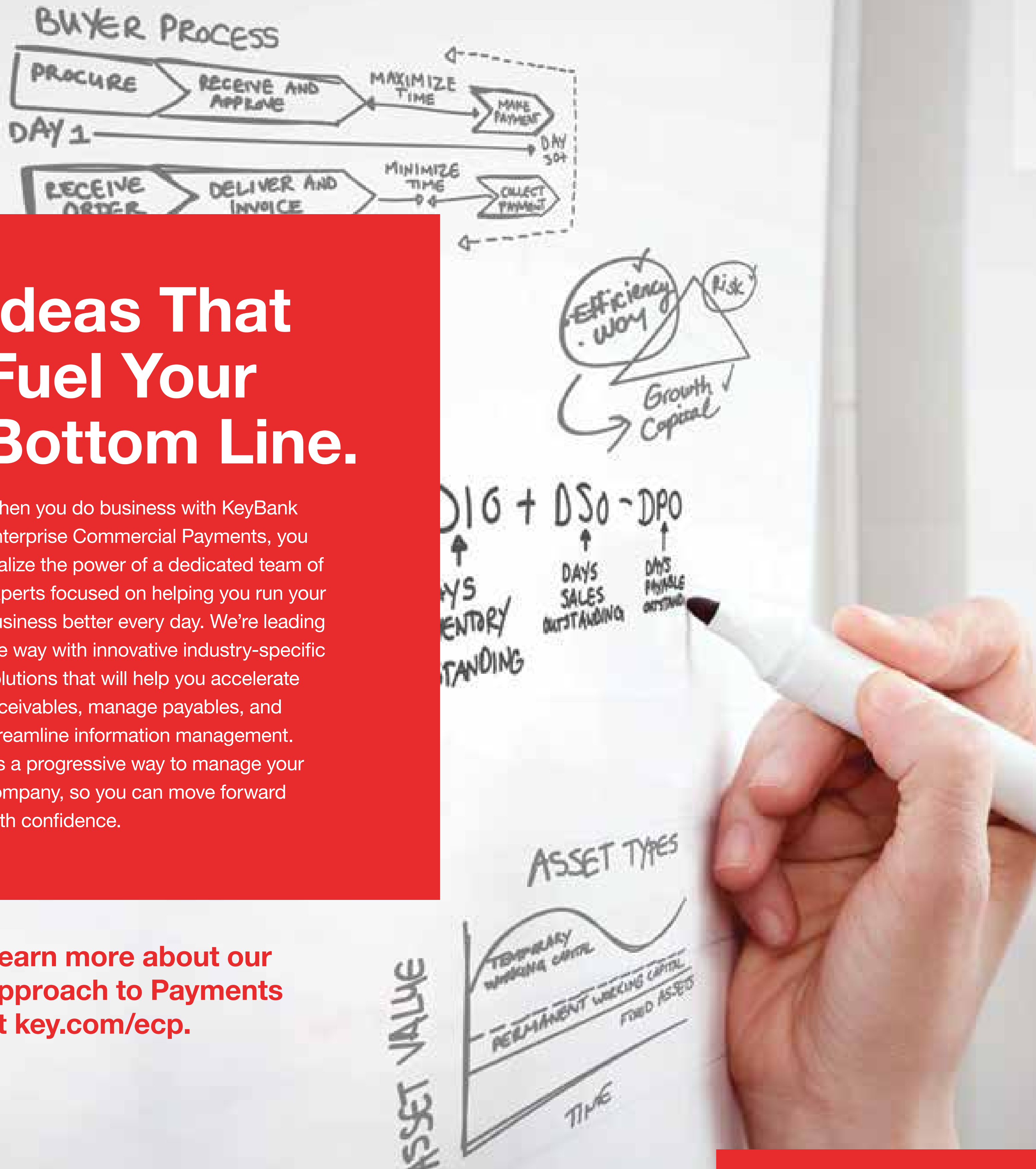
In the United Kingdom, for example, the Joint Money Laundering Intelligence Taskforce (JMLIT) links government agencies, law enforcement bodies, and 25 major U.K. and international banks. JMLIT's approach is based on a model of "collaboration, collective ownership and prioritization"[12] to combat high-end money laundering. 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 U.K. 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 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



Ideas That Fuel Your Bottom Line.

When you do business with KeyBank Enterprise Commercial Payments, you realize the power of a dedicated team of experts focused on helping you run your business better every day. We're leading the way with innovative industry-specific solutions that will help you accelerate receivables, manage payables, and streamline information management. It's a progressive way to manage your company, so you can move forward with confidence.

Learn more about our approach to Payments at key.com/ecp.

KeyBank

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 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. 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.[24] 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.

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 government and the private sector. The U.K.'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.

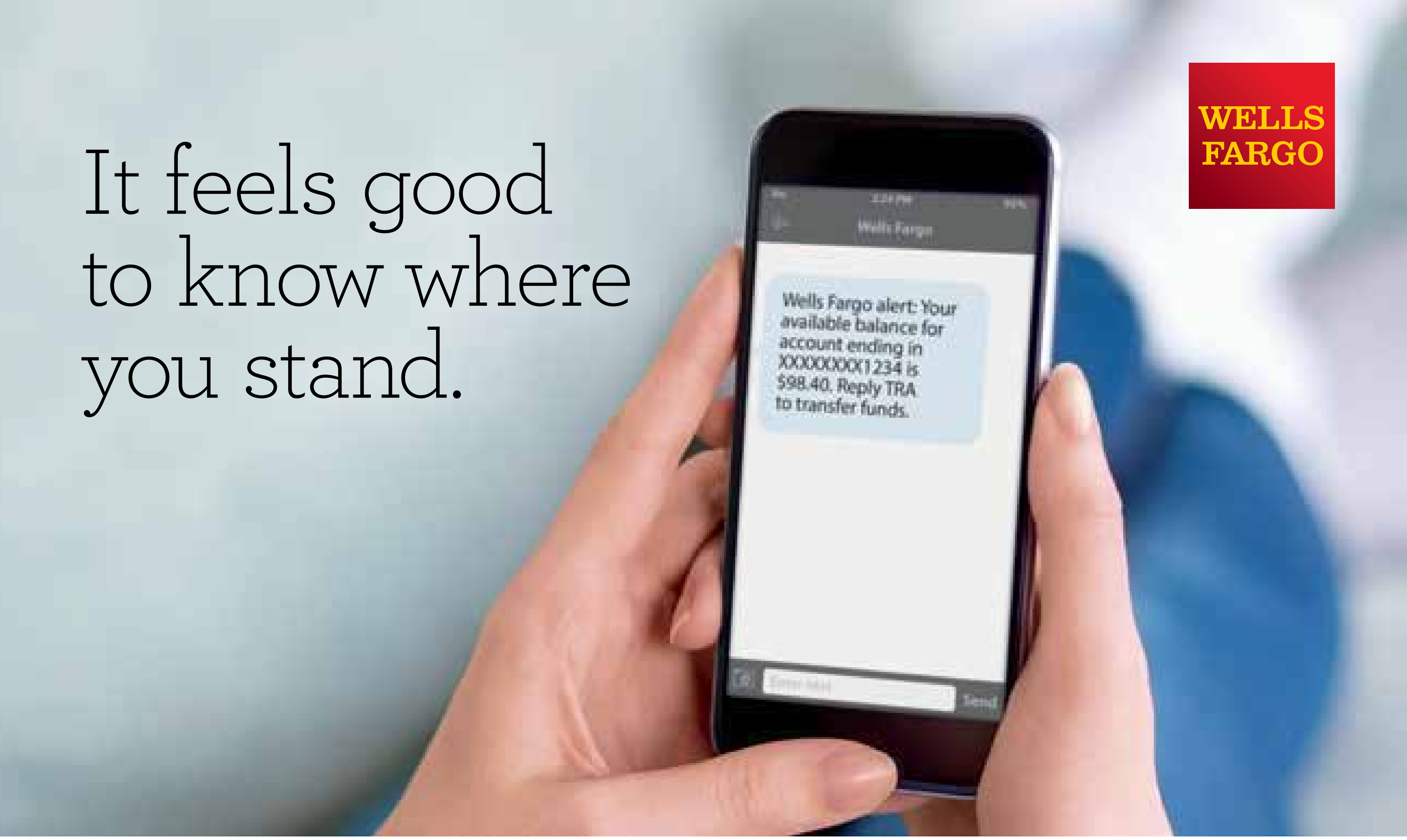
CONCLUSION

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're 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. ■

ENDNOTES

Due to the extensive list of citations, please visit the article on the Q3 2016 Banking Perspectives *page to see the full list of references and web links:*
theclearinghouse.org/publications/banking-perspective

It feels good to know where you stand.



Wells Fargo wants you to feel confident managing your finances. Here are just a few ways we can help.

A conversation about financial needs

We'll spend time understanding your financial needs and discussing your accounts and options. And you'll leave with a printed summary of what you and your banker did that day, including what was discussed and the choices you made.

Welcome email

Within about an hour of opening a new checking or savings account, you'll receive an email confirming what you chose, some important information about your deposit products and services, what to expect next, and how to easily get in touch with us if you have any follow-up questions.

Low balance alerts

You can avoid surprises by setting up balance alerts. You will receive a text or email whenever your account balance goes below an amount you've set.

Customer commitment

We want to make sure you have the account that you feel best meets your needs. And because of that, we wait 64 days before charging a monthly service fee for your new checking or savings account, giving you time to meet the requirements to avoid the fee. If you're not happy with your account, let us know. We will close it, or help you find one that works for you. Depending on how you use your account, there could be other service fees for specific transactions, and we're happy to explain or answer questions you have at any time.

For more information, visit wellsfargo.com

Together we'll go far

STRENGTHENING THE RISK-BASED APPROACH

THE RISK-BASED APPROACH IS EXTREMELY USEFUL, BUT REGULATORY, MEDIA, AND BUDGET PRESSURES HAVE HURT ITS IMPLEMENTATION AND EFFECTIVENESS ON MANY LEVELS.*

BY BOB WERNER AND SABREEN DOGAR, HSBC

THE RISK-BASED APPROACH (RBA) is widely used across the private and public sectors to manage risk. The financial industry began to adopt this approach for managing financial crime risk because of strengthened anti-money laundering (AML) legislation, such as the U.S. Bank Secrecy Act (BSA). The essence of the RBA is to proportionally allocate resources commensurate with varying levels of risk. Tools such as risk assessments, risk models, and risk appetite statements are used to drive an effective RBA by showing a business where its risk lies and helping it to monitor the effectiveness of its controls. The RBA is used to ensure risk mitigation efforts are prioritized toward highest risk areas. The concept is simple and sensible – in a world in which resources are often limited, the correct application of this approach ensures that the use of systems, controls, and people to mitigate financial crime risk is as effective as possible.

Successful implementation of the RBA, however, isn't simple. Despite guidance from regulatory agencies, as well as most financial institutions basing their financial crime compliance frameworks on the RBA, the industry seems to be, in practice, drifting away from adherence to RBA principles. There are several reasons for this, many of which are interconnected and form a vicious cycle.

But first we need to recognize the consequences of losing RBA principles. One outcome is that we may become overly cautious and attempt to implement compliance programs designed to mitigate all financial crime risk. Aside from the fact that it's not possible to eliminate the risk of financial crime and still have a functioning financial system, even an attempt to implement such an approach would be too expensive for most firms, not to mention off-putting to many customers, who would likely find the requirements placed on them too burdensome and would take their business elsewhere. Being overly cautious may also lead to oversimplified risk management efforts, such as de-risking.

The other, more common, outcome is the tendency to become too reactive with risk management efforts, leading to a detrimental misallocation of resources. In recent years, with heightened attention by regulators, lawmakers, and the media, financial institutions are overlooking RBA principles and instead shifting their limited resources to "put out fires," or demonstrate responses to financial crime risks that simply happen to be hot topics.

This is not to say that firms should be rigid in their approaches to financial crime risk management. Instead, flexibility is key because risks are always changing, and firms must adapt. Assuming a bank's RBA is sound, changes to the financial crime risk environment will become evident and warrant a shift of effort and resources to the highest and most pressing risks. Not investing in the tools and processes that underpin a sound RBA – or, even worse, ignoring the RBA altogether – means that firms may not focus enough attention on areas where financial crime risk is greatest.

Given the potentially significant consequences, why are we witnessing the diminishment of the RBA?

FEAR OF ENFORCEMENT ACTIONS

Enforcement actions (EAs) play a critical role in deterring financial crime risk mismanagement, negligence, and misconduct. It is appropriate that there are consequences for misconduct, and it's also beneficial that those consequences often result in an entity correcting

*TO READ THE UNABRIDGED VERSION OF THIS ARTICLE, VISIT:
THECLEARINGHOUSE.ORG/PUBLICATIONS/BANKING-PERSPECTIVE

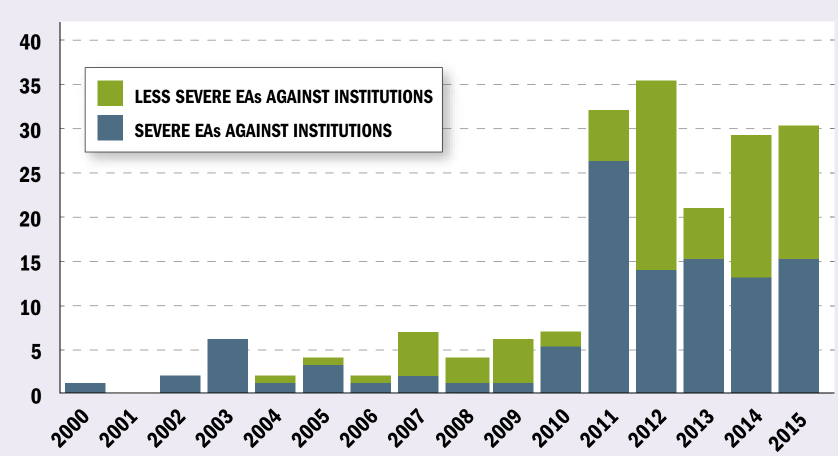
deficiencies and improving its compliance program. As a result, enforcement can also have a broader, positive effect of helping to drive best practices across the industry. However, it's understandable that the industry is concerned about EAs, as they are punitive on many levels: They can be costly, resource-consuming, and can damage reputations.

Yet in recent years, several high-profile EAs have come with record-breaking fines, causing what has long been a concern to swell to an almost palpable fear. The public perception is that hefty fines are shrugged off by large banks as just "the cost of doing business." However, that is not the case. The past few years have seen the banking industry engage in serious cost-cutting measures. As such, banks are in no position to take regulatory fines lightly.

According to a study by Deloitte, the use of EAs by regulatory agencies has increased both in number and severity during the past decade. The data shows that not only have EAs been issued against large banks much more often (Figure 1), but also that BSA/AML deficiencies are one of the top reasons for severe penalties (Figure 2).[1]

Moreover, there are additional challenges after an EA is issued. This is because an EA is almost always a promise of follow-up exams by multiple regulators, as well the need to fulfill myriad obligations. Falling short on the obligations can mean further enforcement actions, additional fines, or even criminal liability and prosecution.

FIGURE 1: NUMBER OF ENFORCEMENT ACTIONS AGAINST LARGEST INSTITUTIONS



SOURCE: SNL FINANCIAL; DELOITTE CENTER FOR FINANCIAL SERVICES ANALYSIS

For these reasons, enforcement activity and the potential personal liability associated with compliance weigh heavily on the minds of bank management. This fear can have an influence on a bank's willingness to take the risk associated with the RBA, and may even stifle innovation, inhibiting more effective responses.

There is also a concerning notion that banks are increasingly looking to patterns of enforcement activity to determine how to manage compliance matters, to a greater degree than even regulatory guidance.[2] Certainly, paying attention to external activity in the law enforcement realm and taking lessons from other banks' shortcomings is prudent, and is a proactive way to consider whether similar issues may exist internally. In doing so, however, we have to be careful. If our position on compliance is only shaped by responses to enforcement activity, we may, as the saying goes, throw the baby out with the bathwater. Ignoring the output of risk tools and instead simply reacting to enforcement activity may lead to an unsophisticated and ill-informed approach to financial crime risk management.

LEGISLATION, REGS, AND EXPECTATIONS

Banks may also find it challenging to stick to the RBA because of a disconnect between the wording of regulations and the fundamental spirit of the RBA. The RBA isn't meant to be a 100% foolproof guarantee that a financial crime won't occur. Instead, it seeks to inform a firm how it can be most effective given realistic circumstances with a "zero tolerance" tone.

Strict laws can sway financial institutions to take an overly conservative stance on compliance. The best example of this is the de-risking phenomenon, whereby banks are taking more of a "no risk" approach to managing financial crime risk by exiting entire categories of high-risk customers or exiting certain jurisdictions. Although exiting relationships makes sense in certain instances as part of a risk-based program, if misapplied or overused, de-risking can be counterproductive. As a result, regulatory agencies have begun to realize that navigating this arena is a challenge, and they are taking steps to help by issuing clearer guidance as well as endorsing use of the RBA.[3]

Regulators may also show goodwill by not issuing an enforcement action in every instance in which a breach

has occurred. Take, for example, findings of violation (FOVs) issued by the Office of Foreign Assets Control (OFAC) to financial institutions. The FOVs cite breaches of sanctions laws as well as the errors or deficiencies that cause the breaches, but they also provide context and highlight what a firm may have done right, which demonstrates a nuanced understanding of the realities and complexities of a global business environment. When OFAC does issue a penalty, it's typically the result of repeated or egregious violations, or if the root cause is found to be seriously deficient controls, willful misconduct, or negligence.

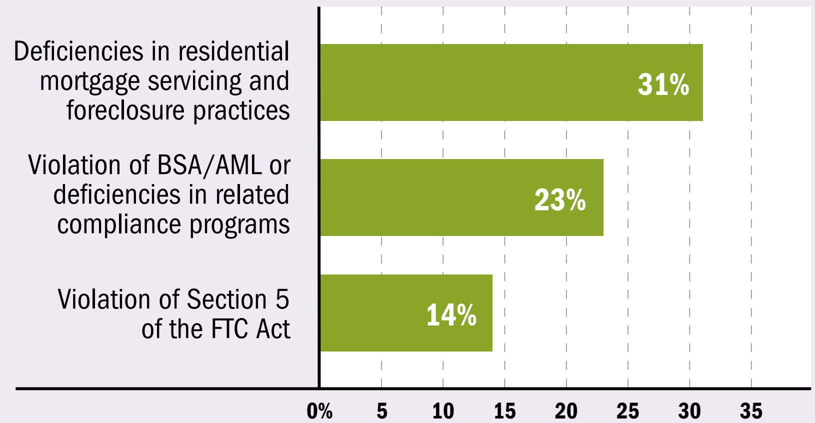
Nevertheless, understanding on the part of regulators that compliance is not a clear-cut matter hasn't slowed the enactment of tougher laws and heightened expectations, further adding to the challenges that banks already face. Take, for example, OFAC's imposition of complex sanctions in the case of Ukraine and Crimea, and the difficulties in navigating the conflicting policies of the amended Iran sanctions. Banks are expected to react quickly to challenging regulatory nuances. The result can be that a financial institution is compelled to take a very simplistic and blunt approach to managing risk.

Given the ever-evolving methods criminals use to avoid detection, lawmakers and regulators are justified in pushing banks to do even more to combat crime. The bar is being set higher, for good reason, but banks are often expected to reach that bar without adequate time to prepare. This predicament chips away at the RBA, as banks can't afford the patience required for risk tools and processes to be applied, their output assessed, and only then used to make changes to compliance programs.

MEDIA COVERAGE

One of the reasons banks may not be given time to strengthen their programs in a deliberate manner is that years of negative press coverage of financial institutions' failures have eroded public trust. To be clear, much of the negative press has been warranted, and it's the media's responsibility to keep the public informed. Negative media coverage often comes hand-in-hand with enforcement actions, and the fear of damage to reputation and the resulting loss of business is also an effective deterrent to bad practice, misconduct, and negligence.

FIGURE 2: TOP REASONS FOR SEVERE ENFORCEMENT ACTIONS AGAINST LARGE INSTITUTIONS SINCE 2008



SOURCE: DELOITTE CENTER FOR FINANCIAL SERVICES ANALYSIS

Aside from reporting on enforcement activity, journalists often investigate potential banking failures based on whistleblowers, data theft, and leaks, among other things, and these stories can have a big impact on how institutions manage their financial crime risk. Investigative journalism has proven to be very effective in drawing supervisory attention to a problem that might otherwise remain under the radar. But the current distrustful attitude toward banks has created an environment in which even an isolated shortcoming can leave the impression that there is a systemic and widespread problem.

It's important to note that the impact of negative press coverage of the financial services sector goes beyond the potential loss of business. A single banking scandal has the power to influence authorities to take action, either by tightening laws or conducting intense exams. Under these circumstances, more failures are likely to be uncovered and enforcement actions issued, which then make more news headlines. This is a vicious cycle, and it detracts from a banks' ability to truly put the RBA into practice.

We're starting to see such a scenario play out with the recent Panama Papers scandal. The International Consortium of Investigative Journalists' coverage of the story has led to public outrage over elites using shell companies to hide wealth and avoid paying taxes. Almost immediately, regulatory scrutiny of the use of shell companies began,[4] and changes to laws are being proposed.[5]

But with this scandal being a result of legislative loopholes and not exactly a banking failure, it will be interesting to see if financial institutions are pushed to act quickly or if they will be given adequate time. Whether laws or banks are to blame likely makes no difference to the public, so our hunch is that it will be the former.

RBA NOT YET MATURE

One final factor behind the diminishment of the RBA is that it may not yet be fully developed in many banks. Although its use is advocated, firms often demonstrate a discomfort with the RBA and thus may be willing to disregard it in certain instances. This could be because key foundational pieces, such as reliable data and a buildup of experienced staff with a solid conceptual understanding of the approach, are not yet fully in place.

> **Enforcement activity** and the potential personal liability associated with compliance oversight **weigh heavily on the minds** of bank management.

Let's consider again the underpinnings of an effective RBA – risk measurement and tracking tools. The output of a risk assessment is used to establish a baseline for other tools, such as a risk appetite statement, which a bank uses to articulate how much risk it's willing to accept in order to meet its objectives. If a risk assessment is an accurate portrayal of the nature of financial crime risk facing an organization, one would expect the risk appetite statement to be set at a level that allows for consumption of some risk. In some cases, though, it appears that banks may ignore what a risk assessment says in favor of simple alignment to regulations. As discussed earlier, regulators recognize that full compliance with zero-tolerance regulations is not necessarily feasible, but oddly, banks might not observe that acknowledgment. Take, for example, the risk appetite statement of a bank that might indicate zero tolerance for sanctions breaches, even though risk assessments (along with common knowledge) tell us that, to a certain degree, breaches must be expected. Ironically, in this case, the bank itself is setting the bar too high.

Finally, we note that a firm may not be comfortable relying on the RBA due to a lack of experience. Financial crime compliance professionals are in high demand, and many financial institutions lament the inability to attract enough talent. Developing new talent will certainly have long-term benefits, but in the short-term, banks must manage their programs comprised of largely inexperienced staff, who may not yet be able to demonstrate the judgment and maturity required by the RBA.

CONCLUSION: THE RISK-BASED APPROACH

One of the first steps toward preserving the RBA is to strengthen the partnerships between financial institutions and regulatory agencies. Open and frequent dialogue between banks and regulators can make certain that banks understand requirements. But this partnership can also help regulators form reasonable expectations of what banks are able to achieve.

A more trusting relationship between regulators and banks can also help with improving the tone of the media, which is a small step toward restoring the public's faith in banks. Failures in the financial services sector will always generate headlines, and when they do, regulators will rightly want to portray their independence and objectivity. But in some cases, despite adequate controls, shortcomings will still occur, as assumed by the RBA. In these instances, it is vital that a regulator credit an institution for good practices or effective controls when publicly disclosing any enforcement actions it chooses to take. Consider the decision by the U.S. Department of Justice (DOJ) to charge a Morgan Stanley employee for violations of the Foreign Corrupt Practices Act in 2012.[6] In its announcement of charges against the employee, the DOJ also highlighted Morgan Stanley's effective control environment and training program. Resulting media coverage of the incident accordingly focused on a sole offender as being responsible instead of the bank itself. This case provided much-needed encouragement to financial institutions, signaling that they will not necessarily be prosecuted for a violation that occurs notwithstanding an effective compliance program – indeed, a compelling endorsement of the RBA.

It's fair to assume regulatory scrutiny of banks won't subside in the coming years, so we can expect the industry to continue paying close attention to

enforcement activity. Again, we should be well informed of activity in the enforcement realm, but we must be careful not to put too great an emphasis on external events and allow them to influence our internal actions. A bank could make better use of EA observations by using them to conduct an introspective check of its risk profile. In other words, before directing resources to show a proactive response, it would be wiser for the bank to first check that it has the relevant data feeding its risk tools and processes, make adjustments if needed, and then allow those tools and processes to indicate whether the bank has the same unmitigated risk.

Investing in improvement of data is critical to bolstering the risk-based approach. There is a clear causal relationship between the quality of a firm's data and the soundness of its RBA. Fortunately, addressing challenges with data is a top priority for several banks and a key regulatory focus.

The bigger challenge regarding data, however, is that of information sharing across the industry. Just like pixels in a digital image, the more data elements we add to our canvas, the clearer our picture of financial crime becomes. But legal hurdles and concerns around data privacy are proving difficult to overcome. While we continue to pursue legal data-sharing agreements, we should also consider tapping into the shared utilities, such as for know-your-customer purposes, that banks are increasingly moving toward to improve efficiency, cut costs, and help reduce customer burden. These utilities present an attractive opportunity to run sophisticated analytics on a vast amount of data. Analytics conducted on data en masse may alleviate some concerns over individual data privacy protection. Ultimately, having a more robust view of financial crime risk can help reinforce each bank's risk profile and, in turn, its RBA, so we believe this avenue is worth exploring.

Finally, there are a number of ways we can address the issue of inexperience. In recent years, several new associations for financial crime compliance professionals have emerged, focused on building knowledge through study, seminars, and conferences. Many of these also provide accreditation or professional certification, which are particularly useful for those new to this industry. Short-term assignments for staff to experience the front lines of business as well as key middle- and back-office roles are critical to developing well-rounded personnel. Such improved understanding on both sides can only help solidify the advocacy and effective implementation of the RBA.

If we can collectively make progress in these areas, then we can save the risk-based approach, at a time when its use has never been more critical. The threat of financial crime grows day by day, and advancements in technology, geopolitical shifts and effects, and increasing global interconnectedness make the fight against criminal networks more complex and challenging. In the face of constant change, the ability to make intelligent decisions by balancing our risks against our resources and limitations will help ensure that our efforts to fight financial crime are sustainable and as effective as possible. If we lose our commitment to the RBA, however, we likely face a future in which financial crime risk management becomes increasingly rule-based and robotic, which will mean that banks and governments will be less prepared to respond in a nimble and focused way to emerging and changing risks. A robust partnership between banks and regulators, the further development and enhancement of industry utilities, and the flexibility and incentive to innovate are all critical to an effective and robust financial crime compliance and risk management framework. ■

ENDNOTES

1 Srinivas, Val, Daniel Byler, Richa Wadhwani, Alok Ranjan, and Vamsi Krishna. "Enforcement Actions in the Banking Industry." Deloitte University Press. December 9, 2015. http://dupress.com/articles/bank-enforcement-actions-trends-in-banking-industry

2 Engen, John. "Drowning in BSA Demands." American Banker. http://www.americanbanker.com/news/consumer-finance/whats-behind-the-uptick-in-bsa-enforcement-1068937-1.html

3 "FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing." Financial Action Task Force. http://www.fatf-gafi.org/documents/documents/fatfguidanceontherisk-basedapproachtocombatingmoneylaunderingandterroristfinancing-highlevelprinciplesandprocedures.html

4 Farrell, Greg, Tom Schoenberg, and Katherine Chiglinsky. "New York Wants Foreign Banks to Hand Over Panama Records." Bloomberg. April 20, 2016. http://www.bloomberg.com/news/articles/2016-04-20/ny-regulator-asks-banks-for-records-linked-to-panama-papers-firm

5 "Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering." European Commission press release. July 5, 2016. http://europa.eu/rapid/press-release_IP-16-2380_en.htm

6 "Former Morgan Stanley Managing Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA." Department of Justice. April 25, 2012. https://www.justice.gov/opa/pr/former-morgan-stanley-managing-director-pleads-guilty-role-evading-internal-controls-required

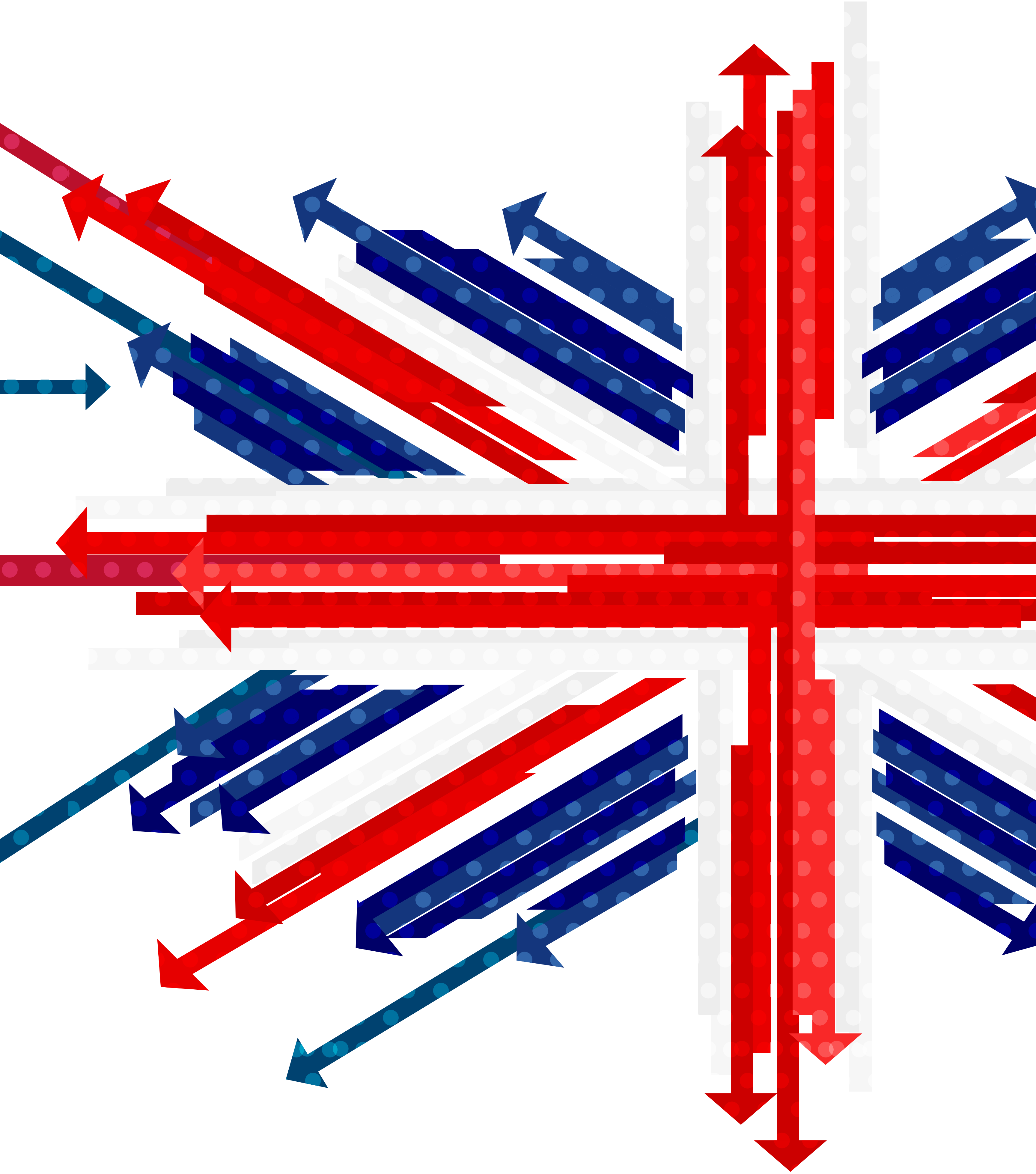
INFORMATION SHARING AND FINANCIAL CRIME:

HAS THE U.K. FOUND THE SOLUTION?

THE U.K.'S JOINT MONEY LAUNDERING INTELLIGENCE TASKFORCE MAY HAVE FOUND A BETTER WAY TO SHARE AML INFORMATION THAT BOOSTS ABILITIES TO TACKLE FINANCIAL CRIME.

BY TOM KEATINGE
ROYAL UNITED SERVICES INSTITUTE

IN THE MOST RECENT QUEEN'S SPEECH, delivered by Queen Elizabeth II in May at the State Opening of Parliament (which marks the formal start of the parliamentary session), the monarch detailed her government's plans for the coming 12 months.[1] Among these plans is the introduction of the Criminal Finances Bill, which will endeavor to "cement the U.K.'s leading role in the fight against international corruption [and] crack down on money laundering and people profiting from crime." The introduction of this bill marks the latest step on the journey the U.K. is taking to overhaul the nation's approach to tackling financial crime, an effort that includes risk assessments, action plans, and the formation of the Joint Money Laundering Intelligence Taskforce (JMLIT). At the heart of these efforts is the belief that better information sharing is needed to overcome the public sector's shortcomings and effectively fight financial crime.



To facilitate improved information exchange, the U.K. Home Office published its Serious and Organized Crime Strategy in October 2013. The Home Secretary introduced the plan as a way to "take action at every opportunity to prevent people getting involved in serious and organized crime; to strengthen our protection against and responses to it; and, most importantly, to pursue the criminals behind it, prosecuting them and disrupting their activities." In sum, the government committed to "the relentless disruption of organized criminals."

The recognition that organized crime (which costs the U.K. at least £24 billion per year) is a threat to national security underpins this strategy. Furthermore, beyond the U.K.'s shores, organized crime groups are seen as key destabilizers of countries that have strategic importance to the national security of the U.K., because they undermine good governance and, in the worst cases, facilitate or engage in terrorism. Although the government built its strategy on the four familiar pillars applied to other areas of national security – that is, pursue, prevent, protect, and prepare – in this case, it added a fifth P: partnership. As the Home Secretary noted, strong partnership, including close collaboration with the private sector, is core to the strategy.

At the same time this plan was introduced, the U.K. government launched the National Crime Agency (NCA), replacing the existing Serious Organized Crime Agency (SOCA) with a broader and more open agency that includes a number of commands dealing with organized crime, border policing, child sexual exploitation, and economic crime. From the start, partnership across government agencies and with the private sector was a cornerstone of the Economic Crime Command's strategy as it aimed to "work with partners and stakeholders across the public sector and the wider U.K. economy, seeking to bring together the most effective range of knowledge, capabilities and skills to reduce the impact of economic crime on the U.K."[2] For the NCA, the challenge presented by financial crime was seen as the "many hundreds of billions of pounds of international criminal money [that] is laundered through U.K. banks every year."[3] Of course, tackling this scourge is beyond the capability of the NCA alone.

Against this background of partnership, outlined in the Home Office's Serious and Organized Crime Strategy and shown by the approach of the NCA, the U.K. government began to update its efforts to tackle financial crime, with one eye firmly on the impending evaluation of the U.K.'s efforts to combat money laundering, terrorist financing, and proliferation financing by the Financial Action Task Force (FATF), slated to take place in late 2017 or early 2018.

This evaluation is one of those regularly conducted by the FATF to determine countries' level of commitment and capability to disrupt financial crime. The FATF was founded in 1989 to combat the rise in the laundering of proceeds of the Latin American narcotics industry through U.S. banks, and it came to significant prominence after the 9/11 attacks on New York and Washington, D.C., when efforts against terrorist financing were added to its mandate. In 2012, the organization concluded a major update and consolidation of guidelines known as the FATF Recommendations, which by then also included a requirement for nations and their financial sectors to combat proliferation financing along with money laundering and terrorist financing.

Before 2012, the FATF's evaluations primarily assessed countries for technical compliance against its Recommendations. That is, they determined if countries had the right laws and governance in place; if terrorist financing was a criminal offence; whether countries had established a financial intelligence unit (FIU) to receive suspicious activity reports (SARs) filed by the reporting sector; whether high-risk businesses such as wire transfers, cash couriers, and NGOs were being appropriately regulated; and so on. But technical compliance doesn't necessarily mean that a country's defenses are effective. Indeed, many countries appear to have passed legislation and set up FIUs – thus demonstrating technical compliance – without actually employing these capabilities in an effective manner.

The FATF expanded its evaluation of countries in 2012 to include not only a test of technical compliance but also an assessment of effectiveness. Based on feedback related to the evaluations conducted since the FATF commenced its fourth round of assessments in 2014, it would appear that countries find it significantly more challenging to demonstrate effectiveness than they do to show technical compliance.

With the challenge of this new methodology in mind, and acknowledging that the U.K.'s architecture for tackling

financial crime was ineffective, the U.K. government set about developing an improved approach for grappling with the financial crime challenges facing the nation.

Speaking at the Royal United Services Institute (RUSI) in June 2014, Theresa May, then the Home Secretary, spelled out the direction she believed this effort should take. May noted that success would depend on developing "effective relationships and information sharing with government departments, regulators, local authorities, the voluntary sector and the private sector" and acknowledged that "we have not always been very effective in this respect."[4] She emphasized partnership between government and the private sector, revealing that she had recently met with the governor of the Bank of England and the chairman of the Financial Conduct Authority, along with chief executives from the financial services sector, to improve the U.K. response to the criminal finance threats. The outcome of that meeting was the creation of the Financial Sector Forum, which, May hoped, would lead to better information sharing.

Over the intervening two years, working in partnership with the private sector, the U.K. government has undertaken a range of activities to enhance its ability to tackle financial crime. Some, such as the completion of a national risk assessment, are common around the world. Others, such as the establishment of the JMLIT, are unique. And central to each one of these initiatives lies the belief that an effective public-private partnership and information sharing are essential to achieving success.

PILOTING THE WAY

No gathering of financial crime professionals, counterterrorism experts, or finance ministry policymakers is currently complete without some presentation or discussion of the U.K.'s JMLIT. Founded initially as a pilot in February 2015 before being memorialized in the government Strategic Defence and Security Review in November 2015 and made permanent in April 2016, JMLIT has formalized public-private efforts to collaborate in tackling financial crime.

As noted by the NCA:

As part of its approach to tackling high-end money laundering, the NCA is prioritizing work to co-operate with the private sector and relevant professional/regulatory bodies in this area. To this end, in February 2015 the Joint Money Laundering Intelligence Taskforce (JMLIT) was established as an NCA initiative created in partnership with the financial sector to tackle high-end money laundering. It has been developed with partners in Government, the British Bankers' Association, law enforcement and over 20 major U.K. and international banks.[5]

JMLIT's objective is to "provide an environment for the financial sector and government to exchange and analyze intelligence to detect, prevent and disrupt money laundering and wider economic crime threats against the U.K."[6] JMLIT focuses at three levels:

- Operational, to enhance collective money laundering detection capability and generate increased prevention and disruption opportunities relating to money laundering activity in the U.K.

> **JMLIT's success** will depend on developing "effective relationships and information sharing with government departments, regulators, local authorities, **the voluntary sector and the private sector."** – *Theresa May (June 2014)*

- Strategic, to increase the U.K.'s public and private sectors' resilience to economic crime.

- Development, to create a more sophisticated U.K. response to money laundering, driven by better informed and capable law enforcement agencies and bank staff.

Key to JMLIT's operation is Section 7 of the Crime and Courts Act (2013), which provides a clear legal underpinning to JMLIT's activities, facilitating the exchange of information between the NCA and the financial sector.[7] Specifically, Section 7 allows that "a person may disclose information to the NCA if the disclosure is made

THE NCA'S SERIOUS AND ORGANIZED CRIME STRATEGY

P PURSUE

Prosecute and disrupt people engaged in serious and organized criminality

- Establish strong, effective, and collaborative organizations
- Develop our capabilities
- Attack criminal finances
- Ensure that effective legal powers are available
- Internationally, improve our own capabilities and our cooperation with others

The NCA will develop an authoritative intelligence picture of organized crime and work with the police and others to lead, coordinate, and support our response. New local organized crime partnership boards will provide support to local policing on all aspects of this strategy. New NCA and law enforcement capabilities will be developed to deal with developments in organized crime, notably the move online. We will legislate on aspects of organized crime. We will increase work against foreign national offenders and refocus the NCA's international network to deal with all crime types.

P PREVENT

Prevent people from engaging in serious and organized crime

- Raise awareness of the reality and consequences
- Intervene to stop people being drawn into different types of serious and organized crime
- Develop techniques to deter people from continuing in serious and organized criminality
- Establish an effective offender management framework to support work on Pursue and Prevent

We will have a new preventative program including more and better education and communications about organized crime, local coordination with existing work on troubled families and gangs, and wider use of interventions (e.g., Serious Crime Prevention Orders). We want to work more closely with the regulators of professions whose members may, wittingly or not, facilitate organized crime activity. We will promote effective lifetime offender management as a framework for both Pursue and Prevent and involving the NCA, regional police units, and police forces.

Reduce Threat

P PROTECT

Increase protection against serious and organized crime

- Protect our borders
- Protect national and local government
- Improve protective security in the private sector
- Protect people at risk of becoming victims
- Improve our anti-corruption systems
- Strengthen systems for establishing identity

We have changed roles and responsibilities at the border and on immigration enforcement. We are building new border capabilities. We will increase work to cut fraud against government and in particular local government procurement. We will share more threat reporting with at-risk parts of the private sector notably on fraud and cyber crimes.

We will provide more information to the public on these issues and also on child sexual exploitation. We will work to restrict circulation of illegal child abuse images. We are revising responsibilities for the investigation and reporting of corruption.

P PREPARE

Reduce the impact of this criminality where it takes place

- Ensure major serious and organized crime incidents are brought to a rapid and effective resolution
- Ensure communities, victims, and witnesses affected by serious and organized crime have the support which they need

We will continue to develop emergency service interoperability to better deal with terrorism and other crimes. We will establish a new unit to coordinate our national response to major cyber attacks including cyber crime.

A theme in this strategy is to provide support to communities affected by organized crime. This is part of all the four main areas of our work. Specific new initiatives are also planned to support victims and witnesses.

Reduce Vulnerability

AIM
Reduce level of serious and organized crime

for the purposes of the exercise of any NCA function." Furthermore, "an NCA officer may disclose information obtained by the NCA in connection with the exercise of any NCA function if the disclosure is for any permitted purpose," with some limited restrictions. In other words, Section 7 creates a legal gateway by which the NCA and the financial sector can communicate to the extent that the communication helps the NCA do its job. The result is that the NCA can harness capabilities across the financial sector in order "to fill intelligence gaps where suspected money laundering crosses multiple financial institutions."[8]

Although JMLIT is still fairly new, there is no doubt that it has already added a valuable extra dimension to the U.K.'s efforts to tackle financial crime by facilitating more effective information sharing and collaboration.

ASSESSMENT AND ACTION

Alongside the trust-building and increasingly effective operation of the JMLIT, the government embarked on a series of initiatives to assess and update the legal and operational architecture underpinning the nation's financial crime-fighting capabilities. The key elements of these initiatives include a review of the U.K.'s SARs regime, a national risk assessment leading to the publication of an anti-money laundering action plan, and plans for the presentation to Parliament of a Criminal Finances Bill that will provide the U.K. with a legal framework for tackling financial crime in the 21st century.

In its most recent report on the U.K.'s SARs regime, the NCA reported that in 2015 up to September, the U.K. FIU received 381,882 SARs from the reporting sector. This number swamps the NCA's capabilities, according to people inside and outside the system. In response to widespread belief that the system was no longer "fit for purpose" and recognizing "that the current system needs to be reviewed to improve our ability to tackle money laundering and the financing of terrorism,"[9] in February 2015 the government announced a Call for Information on the operation of the SARs regime. Specifically, the government wanted to identify the following:

In collaboration with partners in the regulated sector, a more efficient model can be developed that takes into account the increasing number of SARs and the demands placed upon companies and the NCA in operating the regime, and reduces the burden on businesses in complying with the reporting obligations. This Call for Information is seeking views on the ways in which the suspicious activity reports (SARs) regime could be improved, to develop ways of better identifying money laundering and terrorist financing, to streamline the reporting process, and to prevent the abuse of the U.K. financial system by criminals and terrorists.

Responses from across the industry covered issues including the purpose of the regime; the steps to improve the quality of SARs and reducing volume; upgrading the capabilities of the U.K.'s FIU; considering the future of the "consent regime," a unique element of the U.K. SARs regime; and, of course, promoting information sharing. This isn't the place to review the responses in detail, but together with the findings of the national risk assessment, they have contributed significantly to the recently published AML Action Plan.

In October 2015, in line with most other countries' interpretation of the FATF recommendation that states "Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country,"[10] the U.K. published its National Risk Assessment of Money Laundering and Terrorist Financing (NRA).[11] The findings were stark. Although it acknowledged a good understanding of cash-based money laundering by U.K. law enforcement, it noted that "there are significant intelligence gaps, in particular in relation to 'high-end' money laundering." It also noted "the intelligence picture in other areas – such as high value dealers, gambling, and new payment methods – is mixed" and that "the effectiveness of the supervisory regime in the U.K. is inconsistent."

In summary, the NRA noted that "the law enforcement response to money laundering has been weak for an extended period of time. It has not been a priority for most local police forces…" and that "the collective knowledge of U.K. law enforcement agencies, supervisors and the private sector of money laundering and terrorist financing risks is not yet sufficiently advanced." Additionally, the NRA laid out six priorities for the AML Action Plan to address these shortcomings, including – in response to the acknowledgment that "the private sector holds much

of the data needed to succeed in the fight against money laundering and terrorist financing" – a commitment to transform "information sharing between law enforcement agencies, the private sector and supervisors."

Consistent with its earlier commitments, in April of this year, shortly before the prime minister's Anti-Corruption Summit, the government published its Action Plan for AML and Counter-Terrorist Finance.[12] As the Ministerial Forward asserts, the "Action Plan represents the most significant change to our anti-money laundering and terrorist finance regime in over a decade" and, as the NRA indicated, is very much needed. Nineteen actions are detailed, and once again information sharing and public-private partnerships are positioned at the heart of the plan, as it notes:

> *Central to the approach taken in this Action Plan is the recognition of the need to establish a much more effective public-private partnership to tackle illicit finances than has existed until now. Only by bringing together the efforts of law enforcement agencies, supervisors and regulators, and the private sector… can the threat from money laundering and terrorist financing be addressed successfully.*

Specifically, the plan declares "A stronger partnership with the private sector" as one of the four priority areas, envisioning "law enforcement agencies, supervisors and the private sector working in partnership to target resources at the highest money laundering and terrorist financing risks; new means of information sharing to strengthen the application of the risk-based approach and mitigate vulnerabilities; and a collaborative approach to preventing individuals becoming involved in money laundering." Underpinning this effort, as with the support provided to JMLIT though Section 7 of the Crime and Courts Act (2013), is a commitment to explore the introduction of legislation that facilitates better information sharing between law enforcement and the private sector as well as safe harbor provisions to encourage information sharing in the private sector.

But the focus on information sharing by the U.K. government is not confined to the domestic arena. Acknowledging the role the U.K. plays as a global financial center and the risk this presents the nation, particularly banks, accountants, and lawyers in the City of London, the government also wants to lead a push at the international level "to promote better and more effective international information sharing on money launderers between Governments, law enforcement agencies and financial intelligence units, and private sector firms." With the NCA's warning that "many hundreds of billions of pounds of international criminal money is laundered through U.K. banks every year,"[13] the importance of developing an international reach to tackle money laundering and terrorist financing is also a priority for the government that it hopes to pursue via its membership in bodies such as the FATF.

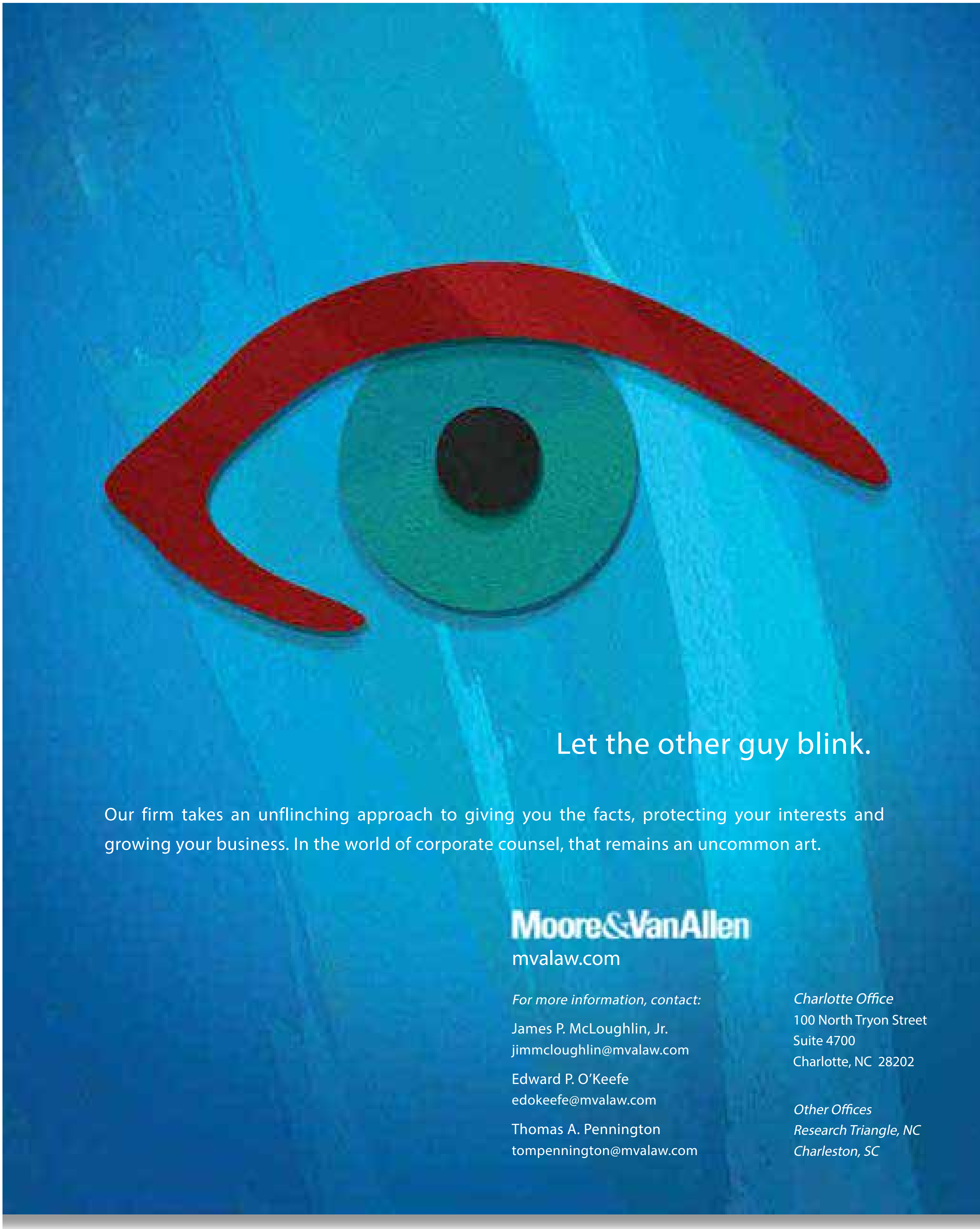
LOOKING AHEAD

At the time of this writing, the U.K. is plotting a coordinated and deliberate course toward delivering a policy, legislative, and operational architecture that meets the challenges posed by financial crime in the 21st century. Central to attaining this goal is the Criminal Finances Bill – a framework that, if implemented, will create a financial crime structure that is modern, collaborative, and effective.

This brings us back to the FATF and the impending U.K. mutual evaluation. The U.K. faces challenges in meeting the technical and effectiveness tests imposed by the impending FATF mutual evaluation. A 2015 paper published by the Centre for Financial Crime and Security Studies at RUSI concluded the following:

> *…policy-makers face significant, but not insurmountable, challenges in the run-up to 2018 if they wish to demonstrate that their approach to AML/CFT [combating the financing of terrorism] is having a demonstrable effect and, in turn, meets the FATF standard. With a more intelligent approach to supervision and compliance, better prioritization of resources and the forming of a coherent narrative across the public and private sectors, the U.K. may well reach the internationally-agreed level set by the FATF. This is, however, not assured.*[14]

Better information sharing between the public and private sectors is the most important factor in improving efforts to stem financial crime, as can be seen throughout the U.K.'s journey over the past three years.



■ Corporate ■ Litigation ■ Intellectual Property ■ Employment & Labor ■ Financial Services ■ Bankruptcy & Restructuring ■ Federal & International Taxation ■ Real Estate ■ Estate & Wealth Planning ■ Privacy & Data Security ■ Energy & Environmental ■ Public Affairs ■ Health Care ■ Global Services ■ Economic Development ■ Transportation

Critics may argue that the government is placing an ever-greater burden on the private sector to make up for its own shortcomings. Why should financial institutions invest billions of pounds in systems and procedures when the authorities seem unable to process, evaluate, and investigate the information provided to them? Although this is a valid question and the authorities need to find ways of engaging with and even rewarding cooperative financial institutions, neither the government nor the regulated sector will achieve the efficiencies and progress that both desire if they fail to develop a more efficient modus operandi. As the AML Action Plan asserts:

> *…central to the success of the Action Plan is a new way of working with the private sector. We need radically more information to be shared between law enforcement agencies, supervisors, and the private sector; and we need to take joint action to disrupt criminals and terrorists.*[15]

> **No gathering** of financial crime professionals, counterterrorism experts, or finance ministry policymakers is currently complete without some presentation or **discussion of the U.K.'s JMLIT.**

Over the past three years, the U.K. has plotted a steady course toward its goal of creating a financial crime-fighting architecture that reflects modern-day risks. No longer is money laundering dominated by "bags of cash in the car park"; rather, it involves high-end practices using shell companies, nominee directors, real estate, and complex offshore structures. Core to this effort is the recognition that the ability of law enforcement to tackle this increasingly sophisticated threat can be significantly enhanced by working collaboratively with the private sector.

Law enforcement can't address the challenges it faces by itself. Acknowledgement of this fact led to the Joint Money Laundering Intelligence Taskforce. The nascent efforts of the JMLIT and the commitment of the government thus far, built on trust and leadership on both sides, suggest that the U.K. may have found a successful formula that overcomes its existing weaknesses allowing both public and private sectors to boost their abilities to tackle financial crime via collaboration and partnership supported by information sharing. And while this remains a U.K. endeavor, driven by a U.K.-specific financial crime and industry landscape, the interest shown in this effort by members of the FATF and other financial crime-fighting bodies suggests that this form of information-sharing partnership will spread. ■

ENDNOTES

1 The Queen's Speech. May 18, 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/524040/Queen_s_Speech_2016_background_notes_.pdf

2 "Economic Crime Command." National Crime Agency. http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime

3 "Money Laundering." National Crime Agency. http://www.nationalcrimeagency.gov.uk/crime-threats/money-laundering

4 "Home Secretary's Speech on Organised Crime at RUSI." GOV.UK. June 10, 2014. https://www.gov.uk/government/speeches/home-secretarys-speech-on-organised-crime-at-rusi

5 "Money Laundering." National Crime Agency. http://www.nationalcrimeagency.gov.uk/crime-threats/money-laundering

6 "Introduction to the JMLIT (JMLIT Toolkit)." Joint Money Laundering Intelligence Taskforce. http://www.nationalcrimeagency.gov.uk/publications/623-jmlit-toolkit-presentation/file

7 "Crimes and Courts Act 2013." UK.GOV. http://www.legislation.gov.uk/ukpga/2013/22/pdfs/ukpga_20130022_en.pdf

8 "Introduction to the Joint Money Laundering Intelligence Taskforce (JMLIT Toolkit)." Joint Money Laundering Intelligence Taskforce. http://www.nationalcrimeagency.gov.uk/publications/623-jmlit-toolkit-presentation/file

9 "Call for Information." UK.GOV. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/518017/SARs_Review_Call_for_Information_FINAL.PDF

10 "The FATF Recommendations." Financial Action Task Force. 2012. http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

11 U.K. National Risk Assessment of Money Laundering and Terrorist Financing https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/468210/U.K._NRA_October_2015_final_web.pdf

12 "Action Plan for Anti-Money Laundering and Counter-Terrorist Finance." UK.GOV. 2016. https://www.gov.uk/government/publications/action-plan-for-anti-money-laundering-and-counter-terrorist-finance

13 "Money Laundering." National Crime Agency. http://www.nationalcrimeagency.gov.uk/crime-threats/money-laundering

14 Wood, Helena. "Destination 2018: Towards the FATF Evaluation of the U.K." Royal United Services Institute. December 2015. https://rusi.org/sites/default/files/20151201_whr_4-15_destination_2018.pdf

15 "Action Plan for Anti-Money Laundering and Counter-Terrorist Finance." UK.GOV. April 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/517993/6-2118-Action_Plan_for_Anti-Money_Laundering__print_.pdf

UNINTENDED CONSEQUENCES OF ANTI-MONEY LAUNDERING

AML/CFT DE-RISKING DISPROPORTIONATELY AFFECTS POOR NATIONS, AND MOVES FINANCIAL CRIME TO SHADOW MARKETS.

BY CLAY LOWERY, ROCK CREEK GLOBAL ADVISORS, AND
VIJAYA RAMACHANDRAN, CENTER FOR GLOBAL DEVELOPMENT

IN FORMULATING POLICY, one important goal of the United States is preventing any sort of financial crime. Money laundering, terrorism financing, and sanctions violations by individuals, banks, and other financial entities are serious offenses with significant negative consequences for rich and poor countries alike. Therefore, efforts by international organizations, governments, and others to combat money laundering and curb illicit financial flows are a necessary step to increase the safety of the financial system and improve security, both domestically and around the world.[1]

Another important U.S. policy goal is allowing finance to flow in the most efficient and competitive manner possible. This helps with global economic growth and leads to more people entering into the financial system in a formal and transparent manner. However, these two legitimate policy objectives have come into conflict, as the policies in place to counter financial crimes may also have unintentional consequences, in particular for people in poor countries.[2] Furthermore, from a national security perspective, today's policies may reduce the transparency of financial flows.

Under the current approach, banks are asked to prevent sanctions violations and assess and mitigate money laundering (ML) and terrorist financing (TF) risks, or face often severe penalties. However, regulators sometimes send mixed signals about how banks should manage their ML and TF risk. This sometimes results in these entities applying simplistic risk assessment methodologies. There may also be a chilling effect resulting from the imposition of fines on some large banks for egregious contraventions of anti-money laundering efforts, combating the financing of terror (commonly referred to collectively as AML/CFT), and, particularly, sanctions laws. These factors, along with others, have led banks to adopt a conservative position with respect to their customers. This includes no longer providing services to firms, market segments, and countries that are seen as being higher risk and that could be the cause of costly future fines, monitoring,

or even prosecutions. In short, banks are engaging in "de-risking" – rather than judging the risks of clients on a case-by-case basis, they cease to engage in certain activities completely.[3]

REGULATORY PRESSURE

Since 2000, the regulatory pressure on financial institutions relating to AML has increased. This is reflected in the number and value of AML-related fines imposed by regulators in the U.S., as Figures 1 and 2 demonstrate.[4] In the five-year period from 2010 to 2015, the number of AML/CFT fines increased more than 65% while the amount of those fines went from $161 million to over $2.6 billion, with a jump to over $15 billion in 2014 alone.

For a variety of factors, individual banks may be acting rationally in not serving certain clients. However, the implementation of AML/CFT policy appears to have created categories of clients whose business cannot justify the compliance costs. The financial exclusion of such clients creates yet another obstacle for economic growth and the alleviation of poverty, especially in poor countries.

There are other factors at work aside from AML/CFT policy and the fact is that the data are too weak to make systemic judgments. However, we do observe strong correlations, and as the IMF recently put it, "Pressure on correspondent banking relationships could disrupt financial services and cross-border flows, including trade finance and remittances, potentially undermining financial stability, inclusion, growth and development goals."[5]

BUREAUCRATIC COMPLEXITY

At the international level, there has been a significant harmonization of legislation that should be counted as a major success for the Financial Action Task Force (FATF), the international standard setter on AML/CFT. At the national level, however, some countries have fragmented regulations. Most importantly, the U.S. has a bureaucratically complex regulatory environment.[6]

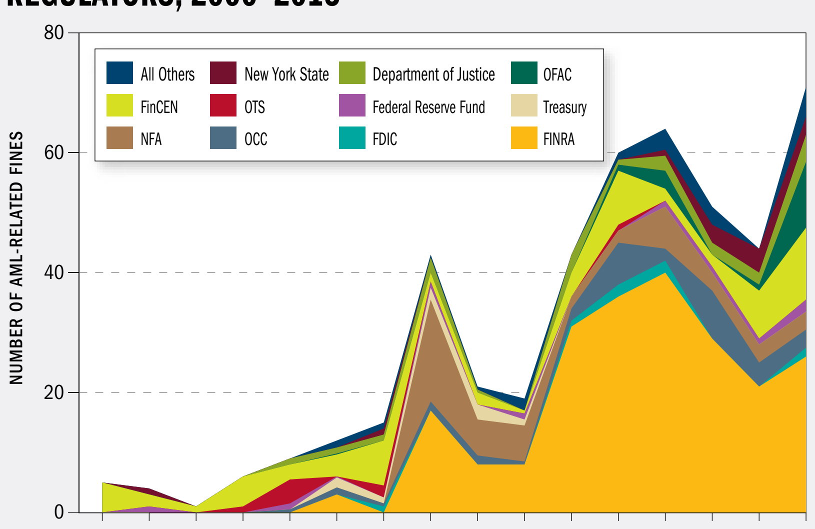
State-level enforcement and regulation add to the total. This creates a challenging environment for financial institutions. Anecdotal evidence suggests that the European regulatory environment is equally, if not more, complex, despite concerted efforts to harmonize approaches through EU directives. This problem is particularly daunting for smaller firms and especially new entrants, creating barriers to entry that undermine competition.

As well as bureaucratic complexity, financial institutions in the U.S. and elsewhere are acting under a degree of uncertainty that arises from the process of interpreting and reconciling regulatory enforcement actions and policy statements. For example, in June 2014, the Office of the Comptroller of the Currency (OCC) published an enforcement action against Merchants Bank of California that contained broad statements indicating that the bank needed to treat all of its money services business (MSB) clients as high risk and take a number of extraordinary measures when dealing with them. When the bank, which was servicing Somali remitters, later left the MSB business entirely, the Somali community in the U.S. was left without a reliable channel controlled by ethnic Somalis for sending remittances home. On the other hand, in November 2014 the OCC issued a statement asserting that it does not characterize all money services businesses as uniformly high risk (see 2).

CORRESPONDENT BANKING RELATIONSHIPS

Correspondent banking relationships are valuable to the global economy, enabling trillions of dollars of cross-border transactions every day in order to facilitate economic activity such as remittances, foreign exchange, and trade finance. Despite this, a number of industry and government surveys of banks have suggested that a substantial number of links between banks have been severed in recent years.

FIGURE 1: NUMBER OF AML-RELEATED FINES BY U.S. REGULATORS, 2000–2015



Source: Data compiled from ACAMS reports of enforcement actions.[7]

A survey carried out by the World Bank in 2015 found that 75% of large global banks are withdrawing from correspondent banking relationships. The World Bank also found that local banks from around the world reported that the termination of correspondent banking relationships was – by far – led by U.S. banks.[8] In the 2014 ICC Global Trade and Finance Survey, 30% of respondents indicated they had recently dropped correspondent relationships.[9] The Society for Worldwide Interbank Finance Telecommunications (SWIFT) provides further evidence.[10] SWIFT documents a significant decline in correspondent relationships between the top 80 payments banks and the American, Europe, the Middle East, and African regions since 2005 (SWIFT 3.0).[11] In a network analysis of SWIFT single-customer credit transactions, Cook and Soramäki note that the majority of links lost in the payments network since 2007 have been to offshore banking sectors, often considered to be high risk.[12]

A desire by banks to reduce regulatory risk and related compliance costs appears to be driving the reduction in the number of correspondent banking accounts. Many regulators ask that banks give these accounts special scrutiny. In the U.S., the enhanced regulatory focus on correspondent banking began with the introduction of the USA Patriot Act,[13] which requires banks to perform special due diligence for foreign correspondent accounts.

While FATF has recently stated that knowing your customers' customers (KYCC) isn't always necessary, a large number of banks and other institutions continue to make this costly effort.[14] SWIFT's new KYC Registry is geared toward facilitating data sharing and making the KYCC concept less expensive and more manageable over time.[15, 16]

As the onus on banks to do enhanced due diligence on correspondent links has increased, so have the costs of getting it wrong. In the U.S., a number of the large fines handed down to banks have been due to failed correspondent banking procedures. In 2014, the OCC fined JPMorgan Chase $350 million for not implementing an "adequate BSA/AML program for correspondent banking."[17]

Finally, more and more countries are being labeled as high risk. The FATF regularly adds or removes countries from its High Risk and Non-Cooperative Jurisdictions list.[18]

While FATF only recommends active counter-measures in the most extreme cases, being added to the list is a signal of high risk. The Financial Crimes Enforcement Network (FinCEN) notes that movement of funds through a listed country could be a sign of terrorist financing activity.[19]

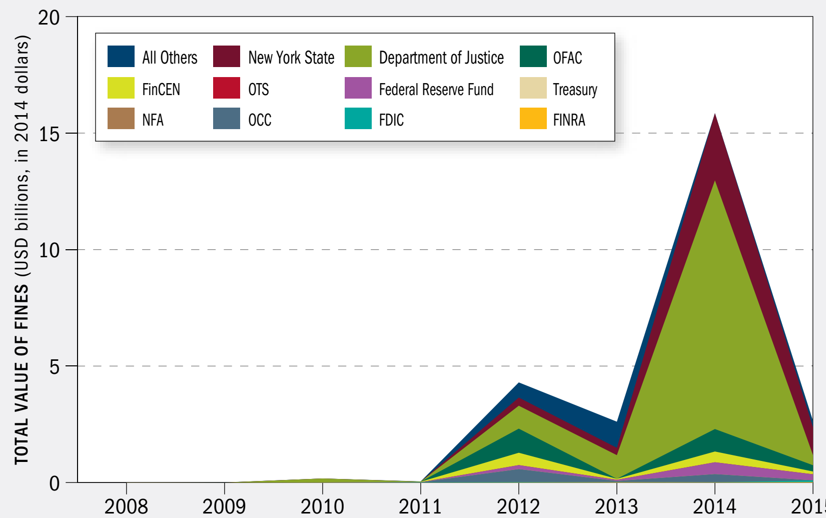
Evidence supports the theory that these factors are causing a drop in correspondent banking. The ECB report specifically mentions compliance costs as a driver of this behavior: "KPMG estimates that global annual expenditure is likely to exceed US$10 billion in the next two years, as billions more pounds, US dollars and euros are been spent building ever-more extensive risk and compliance departments."[20] The ICC Global Trade and Finance survey reveals that 68% of correspondents have had to decline transactions because of AML concerns, with 31% reporting having to terminate whole relationships in the past year.[21]

For many banks, correspondent relationships are crucial for their provision of cross-border services. Furthermore, if a bank wants to settle a transaction in U.S. dollars, they are required to either be based in a country hosting one of the few U.S. dollar clearinghouses in the world or need to bank with a correspondent in that country.[22]

If banks lose access to their primary correspondent account and can't establish a new one through another bank based in their target country, the bank must rely on a third party that does have access to a correspondent account to process cross-border transactions. These "nested" relationships are inherently less transparent, as they force correspondent banks to know detailed information about their respondents' clients in order to detect suspicious transactions. These alternate arrangements are also more expensive.

Aside from the effects on the transparency and cost of financial flows, the degradation of the correspondent banking network has the potential to hamper global trade, as trade finance often uses correspondent accounts for the processing of letters of credit. Over 40% of respondents to the ICC Global Trade Finance survey noted that AML and KYC requirements were a "very significant" impediment to trade finance, specifically in Africa.[23, 24] This has the potential to hurt trade in both rich and poor countries:

FIGURE 2: VALUE OF AML-RELATED FINES BY U.S. REGULATORS, 2008–2015



Source: Data compiled from ACAMS reports of enforcement actions.

If heavily regulated countries are unable to issue letters of credit due to KYC concerns or lack of correspondent connections, then exports from these countries will suffer. Conversely, if banks in these countries are unable to confirm letters of credit issued by banks in "high-risk" importing countries for the same reasons, exports from poor, high-risk countries will also be affected.

RECOMMENDATIONS

Available evidence suggests that banks are engaged in de-risking linked to AML/CFT. However, rigorously examining the extent and precise causes of this de-risking will require better data and institutional cooperation. Reassuringly, very good data either exists within institutions and just needs to be shared, or could be generated with very little investment. In the meantime, further improvements to the system are warranted. Our five key recommendations combine sensible short-term tweaks with long-term investments in data and analysis.

1. **Rigorously assess the unintended consequences of AML/CFT and sanctions enforcement at national and global levels.** *The strength of the evidence detailed in this report requires a rigorous causal investigation of the unintended consequences of AML/CFT enforcement.*

TABLE 1: U.S. REGULATORY AGENCIES RELEVANT TO AML/CFT ENFORCEMENT

FEDERAL BANKING REGULATORS
The Board of Governors of the Federal Reserve System (FRB)
The Federal Deposit Insurance Corporation (FDIC)
The Office of the Comptroller of the Currency (OCC)
The National Credit Union Administration (NCUA)
NONBANKING REGULATORY AGENCIES
Securities and Exchange Commission (SEC)
Commodity Futures Trading Commission (CFTC)
Financial Industry Regulatory Authority (FINRA)
Consumer Financial Protection Bureau (CFPB)
National Futures Association (NFA)
New York Stock Exchange (NYSE)
National Indian Gaming Commission (NIGC)
IRS Tax Exempt and Government Entities Division (IRS-TEGE)
IRS Small Business and Self-Employment Division (IRS-SBSE)
LAW ENFORCEMENT AGENCIES
Drug Enforcement Administration (DEA)
Federal Bureau of Investigation (FBI)
Department of Homeland Security, Immigration and Customs Enforcement (ICE)
Department of Homeland Security, Customs and Border Protection (CBP)
Internal Revenue Service Criminal Investigation (IRS-CI)
U.S. DEPARTMENT OF THE TREASURY
Office of Terrorism and Financial Intelligence (TFI)
Office of Terrorist Financing and Financial Crime (TFFC)
Office of Intelligence and Analysis (OIA-T)
Financial Crimes Enforcement Network (FinCEN)
Office of Foreign Assets Control (OFAC)
Treasury Executive Office for Asset Forfeiture (TEOAF)
U.S. DEPARTMENT OF JUSTICE (DOJ)
Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS)
Counterterrorism Section, Criminal Division (CTS)
National Drug Intelligence Center (NDIC)
Office of International Affairs, Criminal Division (OIA)
U.S. STATE DEPARTMENT
Bureau of Economic and Business Affairs (EB)
Bureau of International Narcotics and Law Enforcement Affairs (INL)
State's Office of the Coordinator for Counterterrorism (S/CT)

- The Financial Stability Board[25] should assess the global AML/CFT and sanctions environment, including the guidance produced by FATF, with a view to reducing unintended consequences.

- FATF should continue to enhance its mutual evaluation methodology to include:

A. *Displacement of transactions from more- into less-transparent channels, which are sometimes informal or processed through lower-tier, less-compliant institutions*

B. *Risks in the whole economy, rather than just in the formal financial sector*

C. *Risks posed to the important drive toward financial inclusion*

D. *Overcompliance at the national level and in particular sectors*

2. Generate better data and share data.

To assess unintended consequences rigorously, private and public sector efforts should generate more and better data.

- The public and private sector, including national financial intelligence units, should collaboratively analyze and evaluate the data available to them around correspondent banking relationships and payment flows in and between countries.

- On behalf of central banks and private institutions, SWIFT, CHIPS, The Clearing House Automated Payment System, Bank for International Settlements, and other entities that may collect data on cross-border transactions and relationships, should consider discussing with their members whether data on bilateral payment flows and the number of correspondent banking relationships between countries should be shared, and if so, how the cost should be covered.

- Specific data should be anonymized to protect proprietary information and safeguards put in place by data collectors, so that even anonymous data is only released to parties intending to conduct analysis in the public interest.

- Governments should make the data that they are using for risk and regulatory assessments available to other jurisdictions and to parties conducting analyses that are demonstrably in the public interest.

3. **Strengthen the risk-based approach.**
   FATF should be congratulated for introducing and strengthening its risk-based approach. However, it needs to be applied more extensively and more consistently.

- FATF should provide a definition of money laundering and terrorist financing risk for its purposes that is consistent with a standardized definition (as provided by the International Organization for Standardization) and existing private sector definitions of "risk."

- FATF should clarify its reasoning regarding transparency and the trade-off of risk in the formal and informal sectors.

- FATF should further encourage simplified due diligence where it is in the best interests of transparency.

4. **Strengthen regulatory and supervisory frameworks.**
   A new IMF report on correspondent banking stresses the need to strengthen and align regulatory and supervisory frameworks.[26] In particular, there needs to be political buy-in to adopt necessary reforms.

- National governments need to invest in supervisory capacity in order to ensure compliance with FATF recommendations and the Basel Core Principles for Effective Banking Supervision.

- National governments need to invest more resources to increase exchange of beneficial ownership information and ensure greater cooperation among national supervisors.

- Sharing information across borders and greater harmonization of regulatory frameworks would likely go a long way toward reducing the level of uncertainty faced by banks.

TABLE 2: 2014 STATEMENTS BY THE OFFICE OF THE COMPTROLLER OF THE CURRENCY

JUNE 2014	NOVEMBER 2014
"As part of [Merchants Bank's] compliance with Paragraph (1) of this Article, the Bank shall also cease and desist from allowing any [MSB, payment processer, foreign or domestic correspondent bank...] from: adding any new Bank products or services; processing any transaction for which the Bank's automated system cannot include the individual transactions in its monitoring or for which the Bank cannot otherwise reasonably ensure the legitimacy of the sources and uses of funds..." – *OCC cease and desist order to Merchants Bank*	"The OCC does not direct banks to open, close, or maintain individual accounts, nor does the agency encourage banks to engage in the termination of entire categories of customers without regard to the risks presented by an individual customer or the bank's ability to manage the risk. "MSBs present varying degrees of risk. "Banks are expected to assess the risks posed by an individual MSB customer on a case-by-case basis..." – *OCC Statement on Risk Management*

5. **Tech adoption and lower compliance costs.**
   Governments, banks, and the World Bank should accelerate the adoption of new technology to facilitate lower cost customer identification, know-your-customer compliance, and due diligence.

- National governments should provide citizens with the means to identify themselves in order to make the reliable identification of clients possible for financial institutions and other organizations.

- National governments should ensure that appropriate privacy frameworks and accountability measures support these identification efforts while ensuring the free flow of information related to identifying money laundering and terrorist financing.

- Financial institutions should redouble their efforts, with encouragement from the FSB and national regulators, to develop and adopt better messaging standards and implement KYC documentation repositories.

- Financial institutions should accelerate the global adoption of the Legal Entity Identifier scheme.

- The World Bank should convene all relevant entities to review the possibility of donor-subsidized third party verification for unprofitable clients. ■

ENDNOTES

1 This essay is based on a report issued by the Center for Global Development in November 2015, http://www.cgdev.org/publication/unintended-consequences-anti-money-laundering-policies-poor-countries.

2 We use the term "poor countries" to describe the countries that the World Bank classifies as "low-income economies" and "lower middle-income economies." These are countries with gross national income per capita of less than $4,125.

3 "De-risking" is sometimes used in this way, and sometimes in a more general sense, to refer broadly to the process of reducing exposure to risk. We employ the more restrictive definition of "de-risking" for clarity, in order to avoid confusion between "good" and "bad" de-risking.

4 For the purposes of this section "AML" is used as an umbrella term, in its broadest possible sense.

5 Erbenová, Michaela, Yan Liu, Nadim Kyriakos-Saad, et al. "The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action." IMF. 2016. http://www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf

6 "Guide to U.S. Anti-Money Laundering Requirements: Frequently Asked Questions, 5th ed." Protiviti Inc. 2012. http://www.protiviti.com/en-US/Documents/Resource-Guides/Guide-to-US-AML-Requirements-5thEdition-Protiviti.pdf

7 Although not a branch of government, the Financial Industry Regulatory Authority, or FINRA, fulfills a regulatory function. It is a self-regulatory organization overseen by the Securities and Exchange Commission that writes and enforces rules governing the activities of more than 4,000 securities firms.

8 "Withdraw from Correspondent Banking: Where, Why, and What to do About It." World Bank Group. 2015. http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2015/11/24/090224b083395501/3_0/Rendered/PDF/Withdraw0from000what0to0do0about0it.pdf

9 "2014 Rethinking Trade and Finance: An ICC Private Sector Development Perspective." Paris: International Chamber of Commerce. 2014. http://www.iccwbo.org/Data/Documents/Banking/General-PDFs/ICC-Global-Trade-and-Finance-Survey-2014

10 SWIFT is an independent, member-owned cooperative society that facilitates secure transactions and information sharing between more than 10,800 financial institutions, including banks, securities institutions, and corporations. The messaging network constructed by SWIFT employs a unified framework composed of business identifier codes (BICs, or SWIFT codes). The use of these codes allows SWIFT to streamline financial messages, increasing their speed, accuracy, and security relative to alternate services. Rather than actually holding funds or securities, and then transferring payments to a different account (electronic fund transfers), SWIFT uses its messaging network to send payment orders from one party to another. These payments are settled by the correspondent accounts that institutions hold with each other, either by virtue of a direct banking relationship or by being affiliated to one such bank.

11 "Correspondent Banking 3.0: The Compelling Need to Evolve Towards a Customer-Centric 'Experience Banking' Model." SWIFT Institute White Paper.

12 Cook, Samantha, and Kimmo Soramäki. "The Global Network of Payment Flows." SWIFT Institute Working Paper No 2012-006. The paper also documents a decline in links to sanctions listed countries, such as Sudan, Cuba, and Iran.

13 Section 312 amends the 1970 Banking Secrecy Act.

14 Schmid, Juan Pedro. "How Much Anti-Money Laundering Effort Is Enough? The Jamaican Experience." Policy Brief 242, Inter-American Development Bank. 2015. http://publications.iadb.org/handle/11319/6904

15 "SWIFT Addresses the Know Your Customer's Customer Compliance Challenge." SWIFT, press release. 2014. https://www.swift.com/insights/press-releases/swift-addresses-the-know-your-customer_s-customer-compliance-challenge

16 American Banker also mentioned this registry. (Reutzel, "'Know Your Customer's Customer' Goes Global," April 27, 2015.)

17 "OCC Assesses a $350 Million Civil Money Penalty Against JPMorgan Chase for Bank Secrecy Act Violations." Office of the Comptroller of the Currency, U.S. Department of the Treasury. 2014. http://www.occ.treas.gov/news-issuances/news-releases/2014/nr-occ-2014-1.html

18 The HNRC process has replaced the NCCT Initiative. That initiative started in 2000 and listed countries deemed to have significant deficiencies and to be "noncooperative" in the context of FATF recommendations. The last country was de-listed in October 2006. The HNRC process is more discriminatory/specific in its classification of jurisdictions' strategic deficiencies, distinguishing between jurisdictions to which countermeasures apply, jurisdictions that have not made sufficient progress or committed to an action plan, and jurisdictions that have made a "high-level political commitment" and action plan to address their issues. The International Cooperation Review Group (ICRG) monitors and reviews these countries, issuing two public documents three times a year.

19 "Aspects of Financial Transactions Indicative of Terrorist Funding." SAR Bulletin 4, Financial Crimes Enforcement Network. 2002. https://www.sec.gov/about/offices/ocie/aml2007/sarbull0102.pdf

20 Keatinge, Tom. Uncharitable Behaviour. London: Demos. 2014 http://www.demos.co.uk/files/DEMOSuncharitablebehaviourREPORT.pdf?1419986873

21 "2014 Rethinking Trade and Finance: An ICC Private Sector Development Perspective." Paris: International Chamber of Commerce. 2014. http://www.iccwbo.org/Data/Documents/Banking/General-PDFs/ICC-Global-Trade-and-Finance-Survey-2014

22 This includes the U.S., Tokyo, Hong Kong, Singapore, and Manila.

23 "2014 Rethinking Trade and Finance: An ICC Private Sector Development Perspective." Paris: International Chamber of Commerce. 2014. http://www.iccwbo.org/Data/Documents/Banking/General-PDFs/ICC-Global-Trade-and-Finance-Survey-2014

24 AML/CFT requirements can also restrict trade finance directly by leading banks to deny letters of credit for which they cannot do sufficient due diligence on the listed beneficiary, an issue also covered in the ICC trade survey.

25 The Financial Stability Board is an international standard setting body for international financial regulations.

26 "The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action." Washington, D.C.: IMF. http://www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf

THE TECH FACTOR

TENSIONS BETWEEN THE LAW AND TECHNOLOGY WILL ONLY DEEPEN, POSING CHALLENGES TO BANKS.

BY GARY M. SHIFFMAN, PH.D., GIANT OAK

RAPID TECHNOLOGICAL ADVANCEMENTS often outpace the ability of decision makers to form policies. This is an age-old problem now besetting bankers, regulators, and law enforcement, and can be seen, for example, in the recent public battles between Apple and the FBI over encrypted iPhones seized in criminal cases. Tensions between legal guidelines and technological advancements are not new, and the law has consistently lagged behind new technology for centuries in cases as diverse as railroads and export controls on supercomputers. As the current unparalleled surge of technological growth in "big data" demonstrates, this tension will only deepen, posing challenges to financial institutions as they attempt to meet regulatory requirements.

Following the attacks of September 11, 2001, the U.S. federal government implemented the USA Patriot Act, which, among other things, strengthened 1970's Bank Secrecy Act (BSA) by instituting increased regulatory requirements and information sharing between the government and financial institutions. Aiming to address concerns over terrorist financing, Section 312 of the Patriot Act "amends the Bank Secrecy Act by imposing due diligence & enhanced due diligence requirements on U.S. financial institutions that maintain correspondent accounts for foreign financial institutions or private banking accounts for non-U.S. persons."[1] As a result, banks are legally obligated to report to law enforcement agencies any information that indicates suspicious behavior.

However, the high costs of BSA compliance as well as the triangulation of the relationship between banks, regulators, and law enforcement (see Figure 1) lead to misunderstandings and misaligned efforts that struggle to meet needs, resulting in a system that's both expensive and inefficient. Fortunately, we can see a path to efficient compliance and high-quality data for public safety and security.

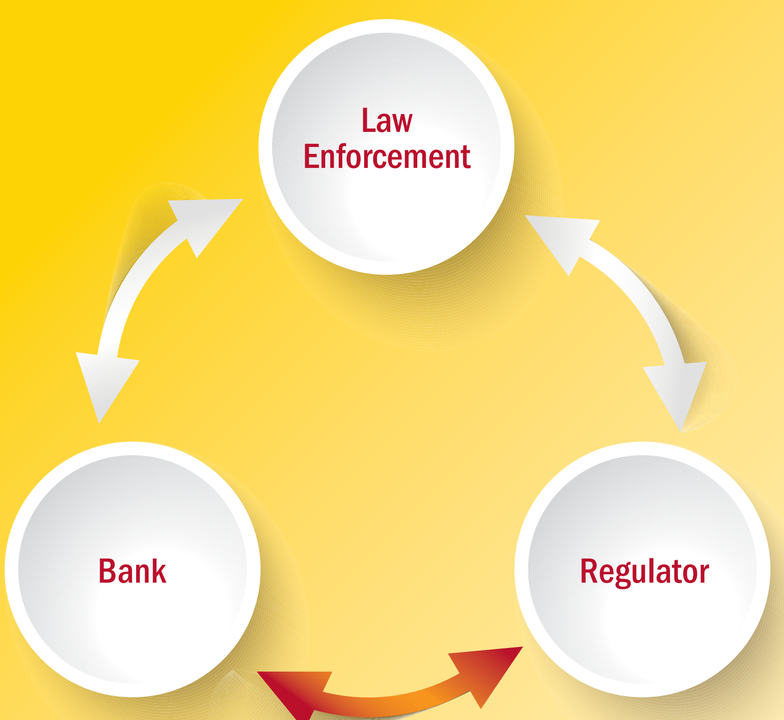
Banks spend significant resources on BSA compliance, often becoming overburdened as a result and losing shareholder value. A Harvard Kennedy School report stated that BSA reporting requirements were among the most cumbersome for community banks.[2] These costs have begun to weigh on larger financial institutions as well, and in 2013 JPMorgan Chase reported increasing its spending by an additional $1.5 billion to manage risk and comply with regulations, "including a 30% increase in risk-control staffing" in 2013.[3] In 2015, Citigroup reported that 59% of the institution's recent expenses savings were "being consumed by additional investments that [the bank was] making in regulatory and compliance activities."[4]

> **The entire system** suffers when law enforcement and technologists **don't participate** in the bank-to-regulator-to-bank discussion.

Future policy efforts must take into account new technological developments in order to craft legislation that works in line with **emerging innovations.**

Beyond rising costs, the entire system suffers when law enforcement and technologists don't participate in the bank-to-regulator-to-bank discussion. Banks tend to follow one another when it comes to compliance technologies for an obvious reason: A banker reduces risk by mirroring the actions of peers. The risk they reduce, however, is the risk of failing to satisfy the regulator and not the risk of failing to satisfy law enforcement by helping them to apprehend criminals.

FIGURE 1: THE LAW ENFORCEMENT-BANK-REGULATOR TRIANGLE



This figure shows the lines of communication between the three key actors: law enforcement, banks, and regulators. The red arrows demonstrate the frequent discussions occurring between regulators and banks, while the gray arrows demonstrate the weaker communication links between law enforcement and the other parties. This breakdown leads to misunderstandings of law enforcement interests and priorities, subsequently contributing to a misaligned focus.

For example, if Bank Z chooses Vendor C for automated compliance solutions, while the majority of the Bank Z's peers use either Vendor A or Vendor B, then Bank Z will increase the risk of perceived poor judgment from the regulator. Moreover, this risk becomes more pronounced to the extent and degree that the regulator has limited knowledge of the technology marketplace.

This herd mentality can be great or terrible. If the technologies resident in the incumbent vendors provide great value – low cost and highly efficient at providing information related to the BSA to law enforcement – then the market works. However, if the existing market technologies, those embedded in Vendors A and B, fail to provide good information at reasonable costs, then the system of incentives can reasonably be described as failing. To be clear: Banks spending considerable resources on technologies do not advance the BSA's legislative goals, while technological evolution provides lower-cost and higher-value solutions. This article seeks to point out the need for attention to this issue.

Ultimately, we have a breakdown in communication among banks, law enforcement, regulators, and technologists, requiring a reassessment of both law enforcement needs as well as banks' technological ability to meet them. Banks want to comply and want their significant investments made in compliance to actually help protect public safety and security, especially as law enforcement investigations continue to increase. Regulators want to help the banks comply while also protecting public safety and security, and law enforcement officials want to do their job with the benefit of the data required by the BSA. All sides maintain good intentions, and this story lacks a villain. We simply need the system of rules and enforcement governing the banks to encourage behaviors to increase efficiency – more deterrence at a lower cost.

This brings us back to the core problem of technology outpacing legal requirements. Future policy efforts must take into account new technological developments in order to craft legislation that works in line with emerging innovations. This requires regulators to better understand technologies for financial institutions. Technologies exist that can drive the cost of compliance and risk management down

and improve the quality of data for law enforcement intended by the post-9/11 legislative initiatives.

The simplest solution is to invest in technological solutions by rewarding innovation through a layered approach to compliance. Regulating bodies such as the Office of the Comptroller of the Currency should discourage the herd mentality by awarding only partial credit to banks that use older solutions. On the other hand, financial institutions that prioritize new, innovative technological reporting tools should be rewarded. This layered approach allows regulators to force banks to adapt their behavior by demonstrating that they need to innovate rather than stagnate in order to meet their compliance needs.

Emerging technologies already on the market can help strengthen this process by improving the government's ability to regulate banks, furthering banks' access to relevant data, and providing a tool for law enforcement officials to accurately identify suspicious activity. Technological innovation, especially in big data and analytics, is advancing at a blistering pace, providing consistent opportunities to drive down the cost of compliance and increase efficiency in advancing national security. These tools should strengthen the relationship that ties together regulators, banks, and law enforcement, ensuring regular interaction and a positive feedback loop to further effectiveness.

At the same time, compliance bodies should also reward financial institutions that maintain an ongoing dialogue with law enforcement agencies and provide useful information to law enforcement in investigating money laundering, terrorist financing, and other crimes. Similarly, compliance officials must improve their communication channels with law enforcement. Part of the communication problems stems from the disconnect between agencies, leading regulators to set reporting requirements around what they think law enforcement needs rather than based on direct input from law enforcement. Instead, all corners of the triangle need to better communicate on requirements, appropriate regulations, and potential reporting tools to ensure improved efficiency on all sides. For example, the recent Mid-Atlantic Money Laundering Conference, held in late July 2016, brought together regulators, financial experts, and law enforcement officers to jointly discuss current shortcomings and ways forward. Maintaining opportunities for dialogue such as this conference will prove critical in ensuring continued progress.

Technology underlies all of these topics and can provide massive improvements to the system, but only to the extent policymakers and regulators maintain awareness of innovation and reward responsible adoption of new technologies. For example, GOST was developed in conjunction with DARPA and federal law enforcement, and

> **Technological innovation,** especially in big data and analytics, is advancing at a blistering pace, providing consistent opportunities to drive down the cost of compliance and increase efficiency in **advancing national security.**

it's now available commercially to banks so they can support negative media search requirements. Many other agile technologies sit ready for deployment today, waiting for the market to reward efficiency across all corners of the triangle.

Although the system may seem broken, these opportunities provide hope that working together will lead to a smarter and more sustainable framework. ■

ENDNOTES

1 "USA Patriot Act." Financial Crimes Enforcement Network. https://www.fincen.gov/statutes_regs/patriot

2 Lux, Marshall, and Robert Green. "The State and Fate of Community Banking." Harvard Kennedy School, Mossavar-Rahmani Center for Business and Government. February 2015.

3 "JP Morgan to Suffer $4 Billion Compliance Hit in 2013: Report," Forbes. September 13, 2013. http://www.forbes.com/sites/thestreet/2013/09/13/jpmorgan-to-suffer-4-billion-compliance-hit-in-2013-report/#34f224e43591

"Annual Report 2013," JP Morgan Chase. 2013 https://www.jpmorganchase.com/corporate/investor-relations/document/01-2013AR_FULL_09.pdf

4 Laura Noonan, "Banks Face Pushback Over Surging Compliance and Regulatory Costs." Financial Times. May 28, 2015. http://www.ft.com/cms/s/0/e1323e18-0478-11e5-95ad-00144feabdc0.html#axzz4GUTxRWnQ

AML AND SANCTIONS REFORM:

BY SHARON COHEN LEVIN
WILMERHALE

IT IS TIME FOR A SAFE HARBOR from enforcement of the Bank Secrecy Act (BSA) and U.S. economic sanctions. Banks play a vital role in the fight against terrorism and illicit finance, but the government's overreliance on enforcement actions against financial institutions has led institutions to make decisions that are bad both for business and for the collection of financial intelligence. For one, large fines and severe, sometimes criminal, punishments have led institutions to withdraw from risky businesses altogether – so-called "de-risking." The withdrawal of U.S. financial institutions from these markets misallocates resources, lessens the quality of information available to law enforcement, and excludes too many people and companies from the banking system.

As rigorous compliance programs are key to the twin goals of obtaining high-quality information for law enforcement and excluding bad actors, incentives for strong compliance programs and a certification process to determine, in advance, whether a bank's practices meet preset standards are needed. Banks that obtain this certification would be entitled to a safe harbor from enforcement actions. These proposed reforms would improve the collection of financial intelligence and more effectively exclude bad actors from the financial system. Regulators and enforcement agencies would benefit from higher-quality information and stronger compliance across the banking industry; banks would benefit from predictable compliance costs and fewer enforcement investigations and penalties; and society would benefit because individuals and organizations in war zones and poverty-stricken areas would have access to better, safer, and less expensive financial services.

THE VALUE OF FINANCIAL INTELLIGENCE

The role of banks in monitoring for suspicious activity goes back to the 1970 Currency and Foreign Transactions Reporting Act, now known as the Bank Secrecy Act (BSA). The BSA authorized the Treasury secretary to require financial institutions to create reports and records that "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[1] Initially, the BSA required banks only to report certain large currency transactions, but as the war on drugs escalated, Congress passed legislation requiring banks to implement anti-money laundering (AML) compliance programs and to report other suspicious activity. In 1990, the Treasury Department established the Financial Crimes Enforcement Network (FinCEN) as a central, government-wide intelligence and analytical network to support the detection, investigation, and prosecution of financial crimes.[2] FinCEN now has authority to promulgate regulations and to enforce the BSA.

A SAFE HARBOR PROPOSAL

Strong AML and sanctions compliance programs provide valuable financial intelligence to law enforcement and protect the U.S. financial system from abuse by rogue states, terrorists, narcotics kingpins, and other criminals. At a May 2016 Law Enforcement Awards ceremony, FinCEN's director praised cooperation by financial institutions, saying: "Without the valuable information that U.S. financial institutions provide, the significant cases recognized here today would likely never have seen the light of day."[3] Other examples of successful prosecutions based on BSA data are cited throughout the 23 issues of FinCEN's *SAR Activity Review*.[4] There is also evidence that financial intelligence has been helpful in fighting terrorism. In its 2015 National Terrorist Financing Risk Assessment, the Treasury Department noted that financial records and information provided by financial institutions played a key role in the investigation, identification, and prosecution of Faisal Shahzad, who attempted to detonate a bomb in Times Square in 2010.[5]

> **Strong AML** and sanctions compliance programs provide valuable financial intelligence to law enforcement and **protect the U.S. financial system** from abuse by rogue states, terrorists, narcotics kingpins, and other criminals.

ENFORCEMENT AND DE-RISKING

The use of financial intelligence provided by banks might lead one to conclude that the AML regime has achieved some success. But continued success depends upon banks' continuing involvement in markets where money laundering and other financial crimes occur. The current enforcement-heavy approach of the government, however, often discourages banks from this kind of involvement.

Under the current BSA and sanctions enforcement regime, FinCEN and the banking agencies encourage cooperation of the financial sector through the imposition of steep fines. Data from the Association of Certified Anti-Money Laundering Specialists indicates that in 2012 there was a 131-fold increase from the previous year in fines and monetary settlements paid by banks for AML violations, with total regulatory fines and criminal monetary settlements jumping from $26.6 million to $3.5 billion.[6] Many regulators also insist on expensive remedial actions, such as transaction "lookback" reviews or the hiring of an independent compliance monitor, as a condition for settlement. And it seems likely that the threat of enforcement actions drives up the cost of compliance. When KPMG surveyed compliance professionals at the top 1,000 global banks, 78% reported increases in their total investment in AML, with 22% reporting increased expenditures of over 50% during the period 2011 to 2013.[7]

This punitive approach to enforcement has made banks risk averse, causing them to close accounts and exit relationships that would otherwise be profitable, provide financial intelligence for law enforcement, or serve a social good. To protect themselves from penalties and in response to the high cost of compliance, banks are de-risking.

Common targets of de-risking include money services businesses (MSBs), foreign embassies, nonprofit organizations, and correspondent banks. Banks also curtail services in jurisdictions perceived as high risk, particularly those with weak AML regimes or that are home to terrorist organizations or drug cartels. Somalia is a commonly cited example, but the effects are also acutely felt elsewhere in Africa, in Latin America, and in other parts of the developing world.[8] Banks also have been closing banking facilities along the U.S. Southwest border in response to fears about the transmittal of illicit funds.[9]

As its name suggests, de-risking is intended to reduce risk, at least from the perspective of an individual bank. But de-risking actually increases risk overall. It does this in two principal ways, the first of which pertains to financial exclusion. Some MSBs specialize in facilitating remittances from immigrants in developed countries to their families in the developing world. When banks close these accounts, they sever an economic lifeline to communities with limited access to the financial sector. Somalia is particularly vulnerable to changes in remittance flows because 40% of its population relies on remittances.[10] Similarly, Mexico receives $51.1 billion in remittances annually, half of which come from the United States.[11] When U.S. banks close branches and curtail services along the Southwest border, the price of those remittances increases as customers are left with fewer options for sending money to family across the border. Charities and nonprofits operating in conflict zones are also common candidates for de-risking because of fears that they may funnel money to terrorist groups. By further destabilizing already vulnerable economies, financial exclusion may exacerbate criminal activity.

The second way that de-risking increases risk is by shifting higher-risk transactions away from large, sophisticated financial institutions to either smaller, less sophisticated financial institutions or completely out of the mainstream financial system into unregulated channels that are difficult to monitor. Those channels aren't monitored by AML officers and, as a result, no BSA reports are filed with FinCEN and transmitted to law enforcement. Because of this, bad actors are still able to conduct illicit transactions (albeit possibly at greater cost), but it becomes more difficult for law enforcement to identify and monitor them.

Regulators have echoed these concerns about de-risking. FinCEN has focused on MSBs, issuing a public statement that it "does not support the wholesale termination of MSB accounts without regard to the risks presented or the bank's ability to manage the risk."[12] The Office of the Comptroller of the Currency issued a statement indicating that it "does not direct banks to open, close, or maintain individual accounts, nor does the agency encourage banks to engage in the termination of entire categories of customer accounts without regard to the risks presented by an individual customer or the bank's ability to manage the risk."[13]

Britain's Financial Conduct Authority (FCA) has taken a similar position, noting that "the risk-based approach does not mean that banks should deal generically with whole categories of customers or potential customers." Lastly, the Financial Action Task Force (FATF), an international organization that sets global standards for AML, has also doubled down on the importance of a risk-based approach that "does not imply a 'zero failure' approach."[14]

THE NEED FOR A SAFE HARBOR

Although regulators have issued statements discouraging de-risking, multimillion-dollar penalties for AML and sanctions failures continue, leading to the exclusion of good customers from mainstream financial services and hampering law enforcement's efforts to monitor illicit activity. Therefore regulatory reforms centered on certified compliance programs that will directly encourage institutions to maintain strong risk mitigation practices are needed. Coupled with a safe harbor from enforcement liability, financial institutions would be free to serve higher-risk clients, counteracting de-risking and improving the ability of banks to provide intelligence to law enforcement.[15]

The AML regime already contains several safe harbors from civil liability. The BSA protects financial institutions from liability relating to suspicious activity report (SAR) disclosures, and Section 314 of the Patriot Act protects financial institutions from liability for certain disclosures of potential money laundering or terrorist financing. A safe harbor to counteract de-risking would be of a different nature. Rather than offering protection from disclosure liability, the safe harbor would protect banks from prosecution and regulatory enforcement. Either regulators could be prohibited from bringing AML or sanctions enforcement actions against banks that have demonstrated a reasonable ability to manage money laundering and terrorist financing risk, or, instead, penalties for violations could be capped at a nominal amount.

To be effective, the safe harbor would need to satisfy three requirements. First, the program would need to be based on clear standards. That means institutions would need a dedicated and responsible officer overseeing the program; requirements for written policies and procedures; training requirements; an AML and sanctions risk assessment process; internal key risk reporting; and rigorous auditing. A regulation recently promulgated by the New York Department of Financial Services may be a starting point, as it requires AML transaction monitoring and filtering programs to have certain specified attributes.[16]

> **In 2012** there was a 131-fold increase from the previous year in fines and monetary settlements paid by banks for AML violations, with total regulatory **fines and criminal monetary settlements** jumping from $26.6 million to $3.5 billion.

Second, the safe harbor would require a form of external validation. One way to do this is by incorporating safe harbor eligibility reviews into the existing bank examination process. Another approach is to have an independent nonprofit, such as the FATF, develop a certification program to conduct initial, in-depth certifications and periodic recertification. As a final alternative, the same private-sector firms that now provide after-the-fact monitoring services pursuant to enforcement settlements could instead serve in the role of delivering a before-the-fact compliance certification (as is the case now, banks would select a preferred company, if the bank's prudential regulator doesn't object).

Finally, banks would need to feel they were buying real protection from future enforcement. This may be the most difficult aspect of this proposal. Under the current risk-based AML regime, regulators would likely argue that banks that maintain reasonable controls have no reason to worry about AML enforcement; however, banks are likely to continue to fear such enforcement actions. But it seems there is some balance that can be struck. Temporarily reducing or eliminating the threat of sanctions enforcement by Office of Foreign Assets Control (OFAC) for institutions that can demonstrate reasonable controls might be a compromise that both financial institutions and regulators could accept. Similarly, an AML safe harbor that granted several years of immunity

from regulatory actions in all but egregious cases might sufficiently tip the calculus.

There are additional complications, to be sure. The safe harbor would likely have to provide protection from both AML and sanctions enforcement to be effective. The AML safe harbor would be relatively straightforward to implement. While politically difficult,[17] a safe harbor built into the BSA would protect banks from liability vis-à-vis all regulators that enforce the BSA. A sanctions safe harbor would be more difficult to implement because U.S. economic sanctions are subject to a patchwork of statutes and executive orders. But it may be possible to create a safe harbor that would constrain the ability of the OFAC to take enforcement action for minor sanctions violations.

Another challenge would be the need for international cooperation. Large banks today are global, multifaceted financial institutions subject to supervision by multiple regulators in more than one jurisdiction. For large banks that operate across multiple jurisdictions, a U.S. safe harbor would be helpful but may not be sufficient to mitigate the global regulatory risk concerns that encourage de-risking. Implementing an effective safe harbor would therefore require cooperation among banking regulators in multiple jurisdictions to agree on uniform standards for a safe harbor. Such cooperation could be facilitated through bilateral discussions or, perhaps more efficiently, through discussion in a global forum such as the FATF.

CONCLUSION

Investigations and enforcement actions will always be needed in some cases. But the current post hoc enforcement approach to fighting illicit use of the U.S. financial system is unbalanced and ineffective, and, furthermore, counterproductive to achieving the goals of AML and counter-terrorist financing. Additional systemic changes will be needed to fully counteract the forces driving de-risking in the long term. But in the short term, a regulatory safe harbor to encourage financial inclusion could change the fundamental calculus of de-risking and bring higher-risk entities back into the mainstream financial system with benefits to banks, customers, and law enforcement. ■

ENDNOTES

1 Currency and Foreign Transaction Reporting Act, Pub. L. 91-508 §§ 201, et seq. October 26, 1970. Section 358 of the USA Patriot Act of 2001, Pub. L. 107-56, expanded the scope of the BSA to include reports or records that have a high degree of usefulness in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

2 Treasury Order 105-08. April 25, 1990.

3 "FinCEN Awards Recognize Partnership Between Law Enforcement and Financial Institutions to Fight Financial Crime." FinCEN press release. May 2016. www.fincen.gov/news_room/nr/pdf/20160510.pdf

4 The BSA Advisory Group is an advisory panel consisting of representatives from federal regulatory and law enforcement agencies, financial institutions, and trade groups. https://www.fincen.gov/news_room/rp/sar_tti.html

5 "National Terrorist Financing Risk Assessment 2015." U.S. Department of the Treasury. www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf

6 Monroe, Brian, and Colby Adams. "Financial Institutions Paid Sharply More for AML Infractions in 2012, Data Shows." ACAMS. June 4, 2013. http://www2.acams.org/webmail/8572/361337941/2bdb107c-6c33761302f879751d26b0fb

7 "Global Anti-Money Laundering Survey 2014." KPMG. 2014. www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf

8 See, e.g., Saperstein, Lanier, and Geoffrey Sant. "Account Closed: How Bank 'De-Risking' Hurts Legitimate Customers." The Wall Street Journal. August 12, 2015.

Corkery, Michael. "Immigrants from Latin America and Africa Squeezed as Banks Curtail International Money Transfers." The New York Times. July 6, 2016.

"African Money Transfers: Let them Remit." The Economist. July 20, 2013.

9 See, e.g., Glazer, Emily. "Big Banks Shut Border in Effort to Avoid Dirty Money." The Wall Street Journal. May 25, 2015.

10 "Hanging by a Thread: The Ongoing Threat to Somalia's Remittance Lifeline." Adeso, Oxfam, Global Center on Cooperative Security Report. Feb. 19, 2015. www.globalcenter.org/wp-content/uploads/2015/11/rr-bank-de-risking-181115-en.pdf www.oxfam.org/sites/www.oxfam.org/files/file_attachments/bn-hanging-by-thread-somalia-remittances-190215-en.pdf

11 Corkery, Michael. "Immigrants from Latin America Squeezed as Banks Curtail International Money Transfers." The New York Times. July 6, 2014.

12 "Statement on Providing Banking Services to MSBs." Financial Crimes Enforcement Network. Nov. 2014. www.fincen.gov/news_room/nr/pdf/20141110.pdf

13 "Statement on Risk Management," OCC Bulletin 2014-58. Office of the Comptroller of the Currency. November 19, 2014. http://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-58.html

14 "FATF Clarifies Risk-Based Approach: Case-by-Case, not Wholesale De-Risking." Financial Action Task Force. October 23, 2014. http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html

15 The U.S. Chamber Institute for Legal Reform has proposed a similar safe harbor in the context of the False Claims Act. See "Fixing the False Claims Act." Oct. 2013. www.instituteforlegalreform.com/issues/false-claims-act?p=8. "False Claims Act: Hearing Before the H. Subcomm. on the Constitution and Civil Justice of the Comm. on the Judiciary." 113th Cong. 77- 94. 2014. (David Ogden, WilmerHale.)

16 See NYDFS Regs. Part 504. http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf

17 While there may be little political appetite for legislation perceived as making it harder to hold banks accountable, several bills passed by the House evidence will to strengthen AML and anti-terrorist financing legislation (e.g., H.R. 5594) and facilitate remittances to Somalia (e.g., H.R. 5607).


VOCALINK
REAL-TIME ACROSS THE UNITED STATES
...the time is now
At VocaLink we believe that sustainable economies are powered by easy access to and movement of money.
Our experts design, build and operate world-class payment systems that keep money moving. We're proud to play our part in shaping the global payments landscape for the better and support TCH and the US in the journey towards the delivery of an ubiquitous real-time solution.
Our technology will enable banks, businesses and everyday Americans to move their money in an instant.
vocalink.com

BREXIT
Significant Opportunities for a Regulatory Reboot

BY BARNABAS REYNOLDS AND THOMAS DONEGAN
SHEARMAN & STERLING

THE U.K.'S VOTE TO LEAVE the European Union has triggered a change in the political climate and in the way banks and financial markets participants are likely to be regulated in the region. The newfound fondness for the financial sector among political decision-makers is unlikely to presage a return to regulatory arbitrage, which has long been blamed as a cause of the credit crisis. However, the situation presents considerable opportunities for improving the regulatory framework for the sector as a whole.

On Brexit, there is a well-known need for an agreement to be struck between the U.K. and EU on passporting – that is, the facility for financial institutions to provide cross-border services to customers in EU countries – or for some suitable replacement. We discuss the likely shape of such an agreement and its implications below. However, the more important point is that, after Brexit, the U.K. is likely to create an environment for financial institutions that is far more attractive and reflects traditional U.K. instincts to avoid overregulation and to spread economic risks and rewards. Of course, the U.K. will still need to continue those mechanisms that clearly address too-big-to-fail (TBTF) and other matters that arose in the last crisis, in accordance with international standards. However, some of the overly zealous European regulations that came into effect after the credit crunch, which have cumulatively affected return on capital and the ability of banks to perform their functions for the benefit of the economy, could be revisited in the U.K. The U.K. can be adept and swift at deregulating and removing unnecessary red tape, and the U.K. appears already to be considering a lightening of the tax burden.

After the credit crunch, a suite of new financial regulatory measures was introduced, purportedly to address the need to avoid future taxpayer-funded rescue packages, the TBTF issue, systemic risk, and regulatory arbitrage. Before the credit crunch, some countries in Europe had sought to attract business by not rigorously applying rules. Laws and regulations were, in part, a marketing tool. This position was dealt with heavily by the G20 after the credit crunch. A G20-led set of initiatives resulted in a new array of worldwide financial regulation – from derivatives clearing to capital, as well as new concepts (in a global context) such as the liquidity ratio. The Volcker Rule and Vickers/Liikanen reforms were separate initiatives designed for similar ends in terms of reforming bank structures. Legislators have acknowledged that the cumulative impact of this raft of new regulation was unknowable until after the rules were applied. Only now is evidence arising that regulations have in some places gone too far, given the retrenchment of business lines in many banks and consequent effects on competition. Lord Jonathan Hill, the British former commissioner in the European Commission, recently kicked off a process intended to rationalize European financial regulation to some degree – for the first time in financial services in the EU. However, Brexit triggered Hill's resignation and the EU program is now in doubt. An even broader exercise of EU deregulation was proposed in former Prime Minister David Cameron's EU deal of February 2016, which now lies moribund following the Brexit vote. The U.K.'s willingness to deregulate remains, and there is now an opportunity (at least in the U.K.) for a proper reconsideration of whether all of the post-credit-crunch regulation is suitable. The U.K. will have more autonomy in determining the environment it creates for the City of London.

The result won't be a complete bonfire. Post-credit-crunch reforms aimed at regulatory harmonization and mutual recognition of premier regulators are likely to remain. However, measures that don't meaningfully reduce systemic risk, or represent a European addition to international standards, are likely to be up for examination.

THE ONGOING U.K.-EU RELATIONSHIP

Any assessment of the possible new U.K. regulatory framework must be viewed within the context of the ongoing U.K. and EU relationship. For financial services, this requires the U.K. to consider the extent to which it wishes to be able to provide certain services to EU-based customers who don't have places of business in the U.K. This is currently permissible because of passporting.

Various EU laws allow certain banks, brokers, exchanges, fund managers, clearinghouses, and other financial organizations established in the EU to "passport" the cross-border provision of their services into other EU member states without the need for further local regulatory approvals or supervision. Passport rights can also in most cases be exercised by establishing a branch in the other member state, which follows a relatively simple process. Furthermore, passporting does not only apply in the EU. It also applies in the three European Free Trade Association (EFTA) countries (Iceland, Liechtenstein, Norway) that are part of the European Economic Area (EEA), known as the EEA EFTA States. The EU plus the EEA EFTA States comprise the EEA.

The passporting system was founded in the Treaty on European Union and the EEA Agreement, both providing for the free movement of goods, services, and capital.

These concepts have been developed further by the EU by sector, with a particular recent focus on financial services. Similar passporting regimes apply for securities issuers selling their securities, filing accounts, and making other reports connected with their listings. It's worth noting that, even with a passport, some local law issues will apply, particularly consumer protection laws and some contract laws. The local courts may also have jurisdiction and, particularly (though not exclusively) for consumer matters, they can favor their own consumers. So the passport is not a panacea, but it is a helpful regulatory tool.

The passport was not always available in the EU or its predecessor, the European Community. The primacy of home member-state regulation and the current scope of the passport date from 2007. As a result of the ease of obtaining a regulatory passport, lawyers have not applied themselves in recent times to considering whether services provided are truly cross-border. Before 1995, significant cross-border business took place within the City of London without triggering the laws and regulations of other countries since the main customer base was (and still is) located in the City itself. This happened through European counterparties and customers having branches or affiliates in London or by U.K. entities using applicable exemptions under EU national laws for wholesale business, private placements, and so-called reverse solicitation. The whole point of a financial center is that it is indeed a center, where people benefit from face-to-face, local interactions.

In fact, most of the services that U.K.-based entities provide are not cross-border in law, or could be made so with minor amendments. Deposit-taking, in the U.K.'s view, takes place where the books and records of the bank are located. Phoning or emailing overseas customers needs to be more rigorously considered in determining whether it is truly a cross-border provision of services or whether it is merely marketing or a response to an inquiry (reverse solicitation). In many member states, the passport is only needed to avoid marketing restrictions, not regulatory restrictions, raising the possibility of regulated EU-based subsidiaries providing a more limited marketing service to support U.K. operations and not being responsible for the actual provision of financial services. In summary, many, if not most, of the services provided by UK-based financial markets participants do not trigger the need for an EU passport and the fact that the institutions concerned have such a passport anyway is superfluous to their needs.

CONTINUED U.K.-EU-U.K. ACCESS

For situations where the cross-border services passport has truly been necessary, the U.K. needs to consider possible trade-offs when deciding the extent to which it wishes to continue the current access arrangements for the EU's markets. There are two basic models for continuing access. First, there could be a negotiation of some version of the current passporting arrangements. Second, there could be equivalence-based access that arrives at much the same place. This is because most of the passporting regimes for EU financial institutions coexist with a side-by-side regime for third-country (non-EU) access where the regulatory framework of the third country is determined to have a set of regulations equivalent to those in that sector in Europe. These equivalency-based rights provide for access, particularly wholesale market access, for many businesses, including brokers, fund managers, investment advisers, reinsurers, and other financial entities. Equivalence-based rights operate in a similar fashion to the EU passport in relying on the supervision of the home state regulator.

Most notably, the Markets in Financial Instruments Directive (MiFID) II, which comes into effect on January 3, 2018, well before Brexit takes effect, provides for equivalency-based access for EU nonretail investment business. This applies to broker-dealers, investment advisers, portfolio managers, non-bank custodians, and banks' investment businesses, among others. In addition, under MiFID II, U.K. firms can provide wholesale services across Europe once they have established a retail branch in a relevant member state, again subject to certain conditions, including equivalence. This provides flexibility for investment businesses operating from the U.K.

It's important to remember that access needs to be two-way. It needs to apply from the U.K. to the EU and back to the U.K. There are more than 70 EU banks in the City of London, many of which operate through branch passports. The passport overrides the policy applied by the Prudential Regulation Authority that banks or investment firms from other countries operating systemically risky or significant businesses in the U.K. need to do so

through local subsidiaries. The costs required for U.K. subsidiarization by EU institutions could be substantial, mirroring the significant costs imposed by the intermediate holding company requirement for certain foreign banking organizations with the largest U.S. non-branch operations. The U.K. regulators have indicated that they wouldn't apply these requirements to EU institutions going forward, but that assumes that the EU provides for suitable access for U.K.-based institutions.

Cross-border access from the EU to U.K. markets would currently be governed by the so-called "overseas persons exclusion" that allows all firms, both EU and non-EU, to access the wholesale U.K. markets for cross-border business without local regulation. Firms are merely required to comply with the U.K.'s marketing laws. Just like outbound U.K.-EU business, this arrangement doesn't work well for retail business, which remains very state-based and protectionist across most of Europe. The U.K. will have a policy choice to make as to whether to change its current level of inbound access to mirror any U.K.-EU outbound arrangements or whether to take the view that cross-border business is to be encouraged and not to impose barriers.

THE LIKELY WAY FORWARD

It seems doubtful that an acceptable version of the passporting arrangements is capable of being negotiated, given the importance of sovereignty as an issue in the Brexit referendum. Passporting requires that the U.K. applies identical rules in a similar manner to the EU. Two issues of sovereignty arise. The first issue relates to rule-making. EU financial services laws are currently made through the EU legislative process. If legislation is to be applicable in the U.K., then the U.K. would wish to have a seat at the table, which looks like participation in an EU legislative project of a kind that has been rejected in the referendum. Furthermore, it's difficult to see how the U.K. could be protected from being outvoted. Arrangements had been introduced for dealing with eurozone countries outvoting the U.K. within the existing EU construct. But even if something similar were adopted, this doesn't amount to giving the U.K. a veto over proposed rules.

The U.K. also has a fundamentally different legislative approach and legal tradition compared with many EU countries and the European Commission (EC). The

> "The post-Brexit arrangements present **significant opportunities** for the rationalization and reduction of some of the heavy-handed **cumulative effects** of multiple separate legislative and regulatory initiatives."

commission, which has sole authority within the EU to propose legislation, has never repealed financial services regulation. It has only added to or re-enacted regulations. The EC's instinct is to make more and more rules. In addition, various European countries take a protectionist approach to rule-making rather than the free market, deregulatory approach favored by the U.K. After the credit crunch, despite the globally agreed upon need for extensive regulation to resolve too-big-to-fail concerns, many would agree that some EU laws have gone too far. The U.K. would not wish to have to persuade others to come along with it on the reformist path, and to be subject to evolving regulation that is likely to be at odds with its freer market wishes.

The second issue of sovereignty relating to passporting arises from the involvement of supranational bodies. The passport necessitates taking an equivalent interpretative approach to the rules. In order to achieve this, the EU has introduced European Supervisory Authorities (ESAs), which are intended to ensure a consistency of interpretation by national regulators. These agencies don't directly supervise institutions, with the exception of trade repositories. However, they have supranational authority.

The interpretation of EU laws and regulations is also ultimately decided by the European Court of Justice (ECJ), a body many in the U.K. regard as highly politicized such that legal rigor can be sacrificed, particularly in favor of EU integration. The ECJ has made no positive decisions on "subsidiarity," for instance, which was a concept introduced in part at the behest of the U.K. in 1993 to ensure decisions are taken, where possible, at a member-state level.

It is possible that arrangements could be set up where the U.K. courts were the ultimate arbiter on the meaning

of pan-EU rules as applied in the U.K., and the U.K. and European institutions coordinated the application of those rules across the U.K. and Europe together. There could be a joint body of the U.K. and EU established to resolve any differences. However, there are still fundamental issues, in light of the vote, with the U.K. adopting rules coordinated by a supranational body with a view to reflecting some form of combined U.K.-EU set of interpretations – and presumably the same concerns would arise in the EU.

On top of all of this, some in the EU have stated that passporting can't come without freedom of movement for people. It is conceivable that some restriction could be placed on that free movement. For instance, if the U.K. became an EEA EFTA State, it could impose restrictions on immigration in the way that Liechtenstein has done. Whether the other EU and EEA states would accept this and whether any new restrictions would satisfy the U.K. public's concerns over migration is not at all certain.

EQUIVALENCE

As a result of the potential obstacles for maintaining passporting post-Brexit, equivalence-based access requires consideration. This approach involves more work for the U.K. and EU, since it involves a determination on a topic-by-topic basis of how equivalent outcomes might be achieved. There are certain gaps in the coverage of the equivalence regimes that would need to be considered.

Third-country equivalency rights are typically based on three things: the relevant institution being properly supervised in its home country; the legal and regulatory regime, including AML and tax arrangements, of the home country being deemed "equivalent"; and the establishment of cooperation arrangements between the home country and EU states or the European Securities and Markets Authority (ESMA). Some equivalence regimes further require a "member state of reference" to take responsibility for the third-country firm. Countries as culturally and legally diverse as Australia, Bermuda, Canada, Hong Kong, Mexico, Singapore, and the U.S. have all been declared equivalent under the regimes for reinsurance and clearinghouses, and their financial institutions in the relevant sectors have access to the EU single market. For some sectors, such as stand-alone lending or insurance mediation, there is no such equivalence framework yet, but one could be developed based on the existing blueprints.

For the U.K. to fall within equivalency regimes will require cooperation between the U.K. and EU regulators and rule-makers. Regulators know from the credit crunch that harmonized rule-making is essential to manage systemic risks and minimize regulatory arbitrage. The U.K. regulators already work closely with their EU counterparts.

The process of being deemed "equivalent" following Brexit should be reasonably straightforward. There is a fast route and a more negotiated route available. On the fast route, the U.K. would grandfather all existing EU legislation "as is," so the U.K.'s laws would be identical to the EU's, not just equivalent. Going forward, the U.K. could, in dialogue with the EU, gradually move away from current EU laws and develop its own approach. The slower route would involve a more negotiated solution, removing or paring back EU laws that are seen by many to have overreached.

There is much to be said for the slower route. Numerous aspects of financial services regulation are not of systemic importance, and could be done away with without damaging any credible application of equivalence. Examples include the requirement in European Market Infrastructure Regulation for both counterparties to a derivative to report trades; some of the antitrust-driven financial infrastructure access rules in MiFID II, which trespass on the U.K.'s sovereignty to deal with market structure and potentially have negative systemic effects such as the fragmentation of markets; the application of the Basel capital standards to domestic and smaller banks; and the bonus cap, which the U.K. addresses in a different way through longer deferral periods (and which the U.K. even challenged in the ECJ). Further, the Liikanen reforms, which were the EU's answer to the Volcker Rule and the U.K.'s similar Vickers proposals, could be reconsidered in their U.K. application.

Brexit represents a moment for the U.K. to reboot its markets and, in the words of some of its proponents, "take back control." Clearly, in many areas, equivalence discussions will require the U.K. to continue applying the thrust of EU laws. But "equivalent" does not mean "identical." The equivalence route should provide an

opportunity for businesses to adopt a more unique approach within the U.K. to regulation and other topics.

In addition, the U.K. could consider establishing financial free zones, such as the one just established in Abu Dhabi, the Abu Dhabi Global Market. Such zones could be carved out of any equivalence discussions and could be purely for local dealings. An even more business-friendly approach could be adopted in the zones, which could, for instance, be set up in Scotland, Wales, and Northern Ireland.

Equivalence determinations can take time if there are material differences to be considered. This, however, is not a position unique to the U.K. All third countries relying on equivalency determinations for third-country passporting will need to take into account those determinations in formulating their own financial regulatory laws. Equivalency determinations have thus far been highly technical matters. For example, equivalency with respect to the United States for derivatives clearing was delayed while a deal was negotiated on the technicalities of different margin calculations arising from two methodologies of calculation, which are now broadly harmonized.

Although many institutions are sensibly considering **contingency plans**, there are many reasons to **wait and see.**

THE PRACTICALITIES

There are those seeking to prevent Brexit completely. There is a challenge before the U.K. courts seeking to require a vote of Parliament prior to the service of the Article 50 notice. This is despite it seeming fairly clear as a constitutional law question that the government may enter into and terminate treaties under its royal prerogative powers. Article 50 of the Treaty on European Union (the Lisbon Treaty) provides that a state may withdraw from the EU "in accordance with its own constitution." Parliamentary approval will, however, be required for the purposes of amending existing U.K. legislation to implement Brexit.

There is also an issue of which aspects of Article 50 require only a "qualified majority" vote (QMV) – a vote weighted by size of population in each member state – and which aspects default to a requirement for unanimous voting by EU members. Article 50 requires that the EU shall reach an agreement with the departing state "setting out the arrangements for its withdrawal, taking account of the framework for its future relationship with the Union."

The extent to which the future trading relationship must be included within the Article 50 agreement is subject to argument. The agreement that is covered by Article 50 requires a QMV of remaining EU member states to vote in its favor and a majority vote of the European Parliament. It must also be ratified by the U.K. Parliament. This contrasts with the position for new treaties, which require unanimity among member states and in some cases other national referenda. On a plain reading, it would appear that Article 50 is intended to be all-encompassing and for QMV to apply to all aspects. It is difficult to see how the withdrawal arrangements could take into account "the framework for [the U.K.'s] future relationship with the [EU]" unless that framework has been agreed upon as part of the same process.

Finally, unless the U.K. is certain that there will be an adequate transitional arrangement such that businesses can wait until termination has been negotiated before considering their positions, the U.K. should not serve its Article 50 notice at all but should continue current discussions so that there is clarity on the deal.

WHAT TO DO NOW

Although many institutions are sensibly considering contingency plans, there are many reasons to wait and see. Both the U.K. and EU need to come up with a new deal for financial services access that preserves the current access arrangements and potentially relieves (at least in the deregulation-minded U.K.) some of the regulatory burdens currently inflicted upon financial institutions. We expect these outcomes to be achievable. The post-Brexit arrangements present significant opportunities for the rationalization and reduction of some of the heavy-handed effects of separate legislative and regulatory initiatives. There is good reason for financial businesses to be optimistic about the post-Brexit outcome. ■

THREE ARTISTS OFFER INTERPRETATIONS ON THE HISTORICAL PERSPECTIVE OF THE CLEARING HOUSE AND THE ROLE OF BANKS IN THE ECONOMY.

BY RIVKA ARNO, TCH SUMMER FELLOW

Adam Cross, Alexis Hilliard, and Joshua Dean

A panoramic view of the NYAA studio

THE ART OF

"The greatness of art is not to find what is common but what is unique," wrote Isaac Bashevis Singer. Now, three young artists are endeavoring to express what is unique about the banking industry and The Clearing House (TCH). TCH has partnered with the New York Academy of Art (NYAA) on a project that seeks to draw on the inspiration of talented, young artists to portray TCH's history and the role of banks in facilitating payments, economic growth, and job creation. On completion, the TCH-NYAA project will provide four original pieces of art for the reception areas in TCH's Grace Building headquarters in midtown Manhattan.

NYAA graduate (MFA 2014) Adam Cross, one of the artists, is in the process of creating a large, 60-by 96-inch oil painting depicting TCH's Cedar Street headquarters from the 1800s as well as street scenes through various time periods at the Cedar Street location. As the painting moves from left to right, the time frame represented progresses from past to present and into the future, showing the transition of buildings, cars, people, and the introduction of technology. With this transition, the palette of the painting steadily brightens, reflecting growth, innovation, and increased vibrancy in the economy.

Working on this piece has been eye-opening, Cross says. "I took it for granted that every time I buy something, every time I do a transaction,

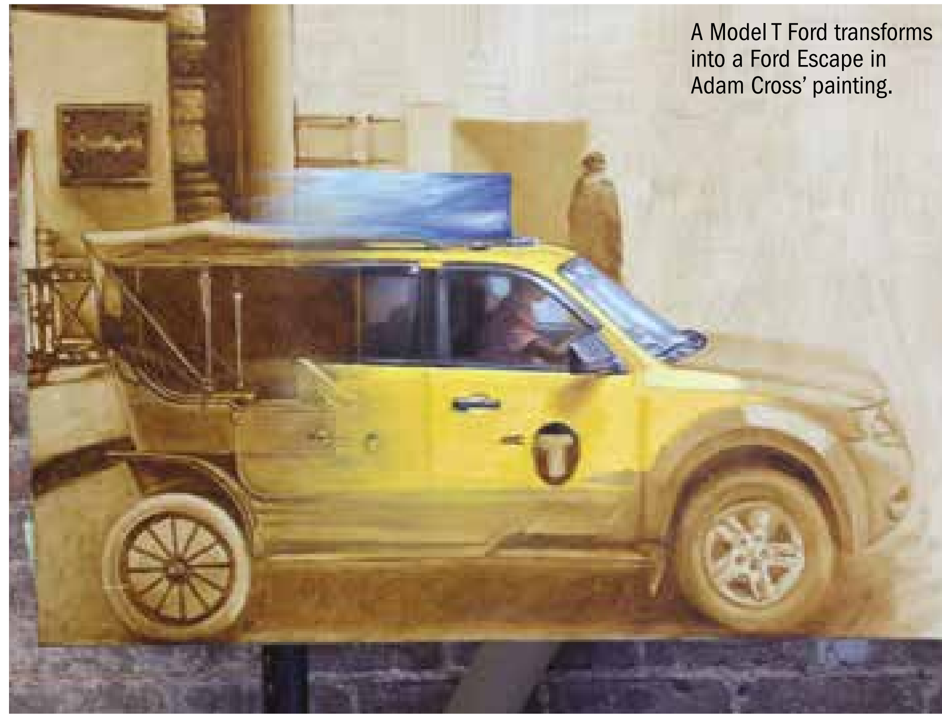
In Alexis Hilliard's collage, countless images come together to form one piece.

BANKING

it just works," he admits. "Now I think about how banks make the economy go and how The Clearing House helps to contribute to that system."

Alexis Hilliard (MFA 2014), another of the artists selected for the project, is also working on a large scale, but in a completely different medium. She is constructing a collage depicting a city through the past 160-plus years, symbolizing not only the growth of the city, but the role that banking and finance have played in the city's evolution.

Hilliard's work also tells the story of how both TCH and society have changed from the 1850s through the 21st century. Hilliard echoes Cross' sentiments about TCH, saying that she "honestly didn't know that much about how banks worked, so it's been interesting learning more about banking and the historical significance of The Clearing House." Hilliard plans to incorporate this historical perspective into her collage, which she is creating through copies of hundreds of pictures gathered from TCH's archives, her own historical research, and current images and photography.



A Model T Ford transforms into a Ford Escape in Adam Cross' painting.

For his part of the TCH-NYAA project, Joshua Dean (MFA 2008) is working on two paintings, one of TCH's original Cedar Street building and a second one of the Grace Building. "These are based upon stereographic pictures that were used to create mock-3D pictures in the 19th century," explains Dean. The first painting is done in an old-fashioned style, while the second will be more streamlined and modern in order to represent both TCH's history and economic progress and dramatic changes in technology. These pieces represent three different artistic media and perspectives, but they show similar interpretations of the role of banking in society and the future of payments. The artworks will be displayed in TCH's offices upon completion this fall. ■

Joshua Dean's two pieces both play on stereoscopic photos that were used in the 19th century. The painting on the left depicts TCH's original location on Cedar Street, while the work on the right is of TCH's current location in the Grace Building in Midtown.

AML: By the Numbers

1,812,248
SARs filed in 2015[1]

$1–2 trillion
Annual global money laundering transactions, an estimated 2% to 5% of global GDP[2]

<1%
Global illicit financial flows seized by authorities[3]

$7 billion
Annual cost in the U.S. alone for implementing AML regulations from the international Financial Action Task Force (FATF)[4]

18%
Banks that have recently experienced AML enforcement actions by a regulator[5]

63%
AML survey respondents who said that regulators should provide additional AML guidance[6]

40%
Companies that have reported exiting a full business line or segment in the past 12 months due to regulatory risk[7]

60%
AML respondents who cite increased regulatory expectations as the greatest AML compliance challenge[8]

1 https://www.fincen.gov/Reports/SARStats
2 http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html
3 Ibid.
4 http://www.pymnts.com/news/2015/the-global-cost-of-anti-money-laundering-efforts
5 http://www.pwc.com/gx/en/services/advisory/consulting/forensics/economic-crime-survey/anti-money-laundering.html
6 https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf
7 http://files.acams.org/pdfs/2016/Dow_Jones_and_ACAMS_Global_Anti-Money_Laundering_Survey_Results_2016.pdf
8 Ibid.

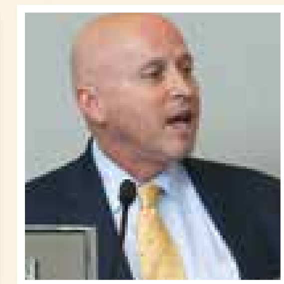
Featured Moments

2016 TCH-SIFMA PRUDENTIAL REGULATION CONFERENCE

Attendees fill a conference hall at Covington & Burling's Washington, D.C., offices to hear a panel at the TCH-SIFMA Prudential Regulation Conference.

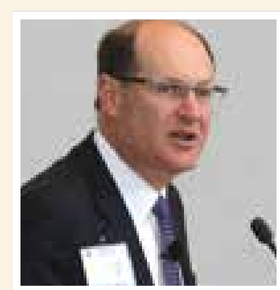
During the panel "Recovery and Resolution Planning," the FDIC's Brent D. Hoyer speaks. Also pictured (L to R): Randall D. Guynn, Davis Polk & Wardwell; Anjan Mukherjee, U.S. Treasury; and Felton C. Booker, Board of Governors of the Federal Reserve System.

President and CEO of SIFMA, Kenneth E. Bentsen, Jr., welcomes attendees and offers introductory remarks.

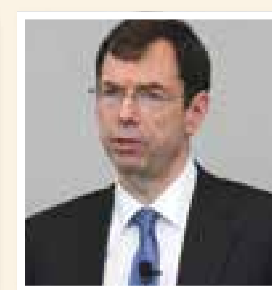


Carter McDowell, of SIFMA, delivers closing remarks at the conference.

Norah M. Barger of the Federal Reserve Board speaks on the panel "Capital, Liquidity, and Funding Regulation," while (L to R) fellow panelists Wilson Ervin of Credit Suisse, Amrit Sekhon of the OCC, moderator John C. Dugan of Covington & Burling, and Adam M. Gilbert of PwC, listen.



Greg Baer, of The Clearing House Association, introduces the keynote speaker, Steven H. Strongin of Goldman Sachs.



Steven H. Strongin, of Goldman Sachs, delivers his keynote presentation at the TCH-SIFMA 2016 Prudential Regulation Conference.

Petr Wagner of the Delegation of the European Union Office speaks on the panel "A Revolution in Capital Markets Structure," while (L to R) moderator Douglas J. Elliott of Oliver Wyman, and fellow panelists Patrick M. Parkinson of Promontory Financial Group, Soo-Mi Lee of Morgan Stanley, Tara Rice of the U.S. Treasury, listen.

Jerome H. Powell, Board of Governors of the Federal Reserve System, discusses his views on the state of prudential regulation while Covington & Burling Partner John C. Dugan listens.

The Clearing House Association's Jeremy Newell speaks during a panel on "Current Regulatory Rulemaking and Supervisory Trends." Pictured (L to R): Michael M. Wiseman, Sullivan & Cromwell; Kieran J. Fallon, The PNC Financial Services Group; Julie L. Williams, Promontory Financial Group; and Robert L. Burns, Chain Bridge Partners.

TCH 7th ANNUAL SPRING LEADERSHIP DINNER

Darrell Walsh, The Clearing House; Beth Mooney, KeyBank; Jim Aramanda, TCH; and Paul Patton, Citibank, at TCH's Spring Leadership Dinner.

Stefan Gavell, State Street Corporation; Pat Parkinson, Promontory Financial Group; and Til Schuermann, Oliver Wyman, prior to the dinner.

Attendees from TCH member banks mingle in the Library at the New York Palace Hotel prior to the dinner.

Attendees converse during the 2016 Spring Leadership Dinner, which was held at the New York Palace Hotel.

Greg Baer, President of The Clearing House Association, welcomes attendees and introduces the keynote speaker, Ben White from Politico.

Ben White, chief economic correspondent at Politico, delivers his keynote speech on Banking and the 2016 Presidential Race.

Following the dinner, attendees from TCH member banks and TCH listen to the keynote presentation delivered by Ben White of Politico.

Finding opportunity in every challenge

In today's fast-paced business environment, it's essential to navigate risk and regulatory complexity.

We can help you transform risk and complexity to your advantage so that you will be better able to anticipate change, be more agile, and more adept at identifying opportunities. All powerful drivers of competitive advantage and growth.

This is what we mean by creating a risk advantage.

Helping your company get the extraordinary done. That's what PwC does.

For more information about PwC's Financial Services Regulatory Practice, please contact:

Dan Ryan
Financial Services Advisory Leader
(646) 471 8488
daniel.ryan@pwc.com

www.pwcregulatory.com

pwc