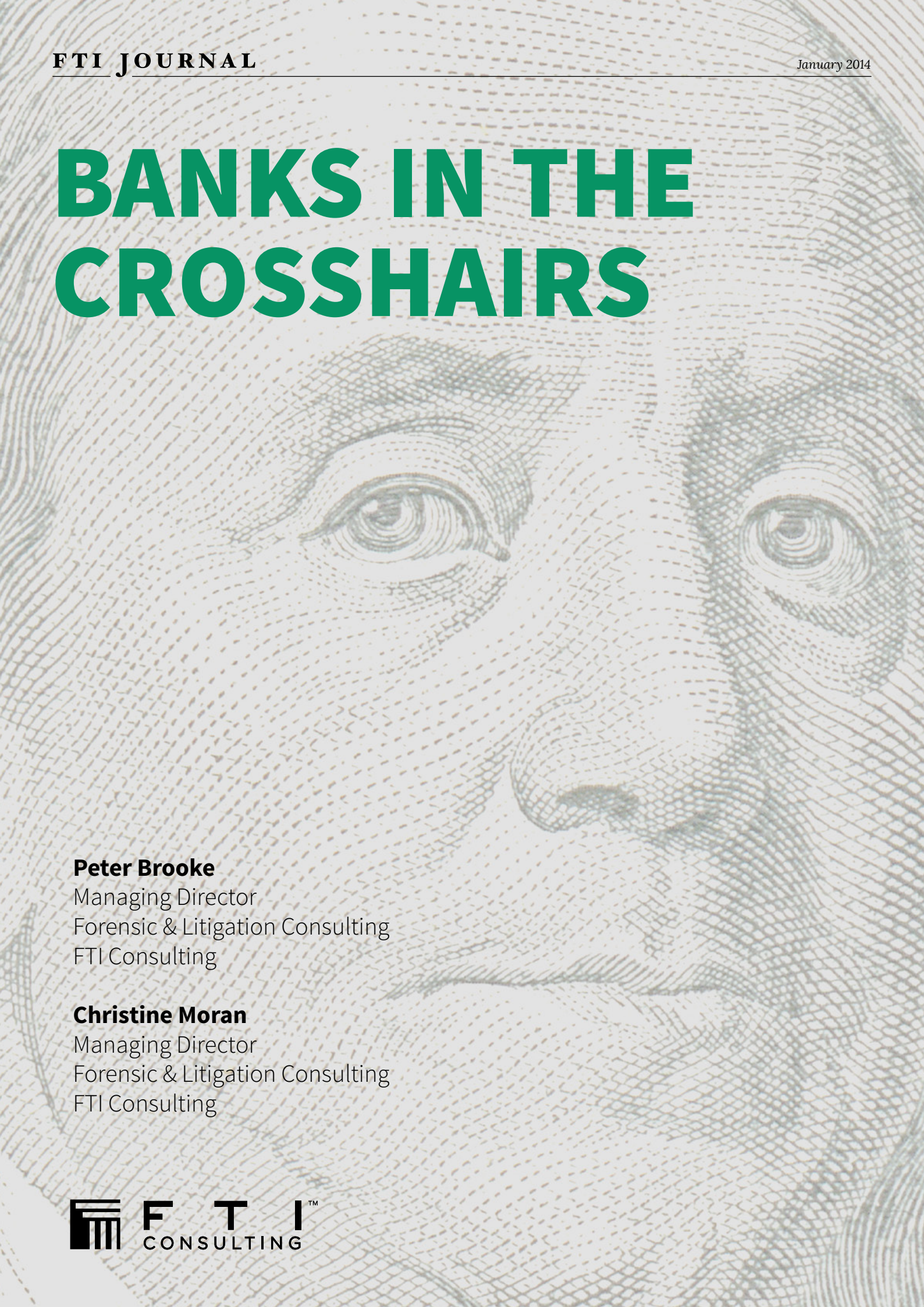
BANKS IN THE CROSSHAIRS



Peter Brooke
Managing Director
Forensic & Litigation Consulting
FTI Consulting

Christine Moran
Managing Director
Forensic & Litigation Consulting
FTI Consulting

FTI CONSULTING™

It's monumentally difficult for banks to ensure that they're not being used by money launderers, terrorists, and other assorted bad guys. But governments increasingly are asking them to do just that, and punishing them severely when they fail. How can banks track customers and regulate transactions more effectively and cost-efficiently?

Governments and regulatory bodies around the world have increased their focus on corruption in international transactions and are targeting criminal activities funded by laundered money. At the same time, these governing bodies are enforcing compliance with international financial sanctions against countries and individuals associated with global terrorism with poor human rights records. This greater scrutiny has led to the imposition of significant fines against many large financial institutions, and now second-tier banks and other financial services companies are finding themselves in the regulatory crosshairs. Beyond the impact of the levied fines, institutions have suffered hard-to-calculate reputational damage and have incurred remediation costs that can make the actual penalties look like pocket change. And sanctions against institutions could prevent banks from conducting business at all — the ultimate consequence could be the withdrawal of operating licenses. Not only is there no sign this trend will abate, U.S., UK and other governments will be holding controlling stakeholders to ever higher standards as global transactions become more complex and difficult to monitor and control. To survive in this environment, the senior management of financial firms, cast in the role as the front-line defense against money launderers and sanctions breaches, must continually up its game by implementing risk-based controls to account for both front-end client acquisition and back-end transaction risk.

Following the Money: No Simple Matter

It has been estimated that there is $2.9 trillion worth of stocks, bonds and derivatives traded in U.S. financial markets each and every day. And according to a 2012 report by the European Central Bank, 2,827 noncash transactions (primarily credit transfers, direct debits, credit card payments and checks, among others) are made by European financial institutions every second of every day of the year. That works out to about 248 million transactions every day and 90 billion in 2012. With the increased popularity of mobile banking, one may presume that figure, already enormous, will grow.

The volume and pace of transactions in global financial markets — magnified and accelerated by new technologies — are mind-boggling. It's easy to see how this makes monitoring both client onboarding and financial transactions monumentally complex. Add to this the easy anonymity received from digital technologies, and one can get businesses such as Costa Rican-based Liberty Reserve, essentially a $6 billion online money laundering operation with a million customers worldwide that processed more than 12 million transactions last year, often for "carders" (people who steal, buy and sell credit cards and personally identifiable information) and other criminals. (Liberty Reserve's founder was indicted, and the operation was shut down in May 2013, but cybercrime experts believe that other businesses already have filled this void.)

While Liberty Reserve primarily was a criminal enterprise (albeit one with many non-criminal customers), legitimate financial institutions all too easily can be used by the bad guys for nefarious purposes.

Punishing the Banks

In recent months, an internal Vatican Bank investigation found that the institution had not been adequately vetting account holders, allowing criminals to launder money and transfer large sums via proxies. Last summer, German regulatory agency BaFin found Deutsche Bank, with more than €2 trillion in assets, laggard in reporting suspicious transactions to the authorities due to inadequate internal controls. Also last summer, a global business advisory firm agreed to pay a $10 million fine as a penalty for removing an anti-money laundering recommendation in a report for a client.

The difficulty of policing transactional activity, as well as violations of international sanctions against countries with ties to terrorism or with poor human rights records, is not lost on governments and regulatory bodies. Consequently, they increasingly are viewing financial institutions as the first line of defense against money laundering and sanctions breaches, seeing that as the only way to keep ill-gotten money out of the financial system and to defund criminals and terrorists. And these governing bodies are enforcing this view with a flurry of fines on banks both for failing to prevent money laundering and for breaching UN sanctions.

A series of fines has been imposed on UK banks in recent years for allowing business to be conducted with countries like Cuba, Iran, Libya and Sudan. U.S. enforcement authorities, flexing their regulatory muscle, have imposed fines for sanctions breaches on Lloyds Banking Group ($350 million), Standard Chartered Bank ($327 million) and Barclays ($298 million). In the UK, the Financial Services Authority imposed a fine of £5.6 million on Royal Bank of Scotland for similar transgressions.

In the United States, the Department of Justice and the Securities and Exchange Commission are using the Bank Secrecy and Foreign Corrupt Practices acts to demand greater due diligence from all parties involved in transactions, holding them responsible for both sins of commission (such as facilitating money laundering or committing sanctions breaches) and omission (such as failing to implement sufficiently strong internal controls). In October 2013, HSBC agreed to a $1.9 billion settlement to resolve charges that it had failed to monitor more than $670 billion in wire transfers, allowing for money laundering, and also had breached U.S. sanctions against Burma, Cuba, Iran, Libya and Sudan.

In short, governments are making it clear that they will not tolerate what they deem to be reckless conduct on the part of financial institutions or what is seen as a weak commitment to abiding by international rules regarding money laundering and sanctions. Governments want senior management to engage and to lead the work in building financial crime defenses.

Financial institutions, however, believe the expectation that they can act as a branch of law enforcement is unreasonable. These organizations, they say, cannot police every transaction or client with 100 percent certainty or make the businesses risk free. Leaders at these institutions say the investment they must make in people, processes and technology, to comply with regulations and avoid being implicated in financial crime, places a massive strain on resources. And, management argues, there is a limited pool of experienced people to draw from to lead, manage and run anti-money laundering and sanctions compliance programs. Consequently, banks are voting with their feet and are pulling out of more risky industry sectors and geographies. Both Barclays and HSBC, for example, decided last summer to stop providing banking services to cash transfer businesses in Somalia for fear that such transactions could be used for money laundering. And while the banks felt they had no choice, demonstrators in London protested that the financial institutions were abandoning people in need, painting Barclays and HSBC — not the relatively invisible and untouchable money launderers — as the bad guys. This is a classic no-win situation.

Manage Risk, Not Money

To satisfy these growing governmental and regulatory demands and to prevent the risk of being abused by criminals and terrorists, financial institutions must improve their risk-assessment capabilities and make that effort an organizational priority.

In short, banks need to get smarter about both client and transactional risk and do more about each category.

This effort must be led from the top. Senior management must set the tone and be fully engaged in establishing the financial crime defenses — the internal controls — that can make the organization less vulnerable both to missteps and the depredations of criminals. Leaders have no choice but to accept their role in the global struggle against financial crime and terrorism and must work consistently to build ever stronger defenses, with risk assessments completed intelligently and thoughtfully and updated regularly. The list of UN-sanctioned countries and politically exposed persons must be monitored continually.

However, given the complexity of global finance and the cunning of criminals, these defenses have to be risk based, with finite resources devoted appropriately to businesses and jurisdictions with inherently higher risk profiles or weaker control environments. And the effectiveness of these defenses must be constantly overseen and reviewed.

Mitigating Client Risk

Financial institutions need to make their client-onboarding rules and processes more rigorous prior to accounts being activated, and those accounts need to be evaluated on a periodic basis thereafter. This requires repeatable risk-based client assessments that can identify:

- Politically exposed persons
- People with criminal backgrounds or connections
- People conducting business in risky jurisdictions and geographies
- Individuals acting as proxies for hidden players

Criminals are continually changing the ways they move money in and out of institutions and are using increasingly complex and opaque structures to hide the true sources, identities and destinations of funds. It, therefore, is essential that financial services firms employ experienced external investigators to establish the identities of high-risk individuals and entities, especially when they come from countries where these data are difficult to acquire and verify.

Mitigating Transaction Risk

Banks should acquire and implement detection technologies that can filter and flag sanctioned or otherwise suspicious transactions. There is a vast array of commercially available transaction-monitoring tools that can hardwire business rules into an institution's systems and define acceptable or unacceptable transactions (such as identifying sanctioned country codes on transfer receipts). These systems can establish thresholds that trigger alerts and automate watch lists for questionable persons and transactions. Some programs also are capable of sophisticated recordkeeping and can produce compliance reporting that can be critical when an institution finds itself in a government's or regulatory agency's crosshairs. But all these processes are only as good as the people who use them. Firms must acquire skilled people to fine-tune the systems, as well as to analyze, assess and act upon the alerts and reports compiled.

These tools and processes, and the human capital that make them work, are necessary for financial institutions to optimize their businesses and steer clear of trouble. Implementation of such systems also is a statement of good faith. Deploying up-to-date tools and processes and staffing the risk-management function as diligently and thoughtfully as possible will make regulators less inclined to punish firms that have proved their commitment by taking these steps yet have run into trouble or made the occasional, unavoidable mistake.

It's Never That Simple

Despite the efforts of the Financial Action Task Force (FATF) to raise the bar for the world's banking institutions and make it more burdensome for people with bad intentions to exploit the financial system, the ease with which money can move from a poorly controlled environment makes it difficult to track even if the domain to which the funds are moving is highly controlled. And once the money has found a home in a good bank, the funds effectively have been laundered.

Complicating that problem is the fact that the FATF can only make recommendations. The agency has no enforcement powers, and not all countries can be counted upon to cooperate. There have been allegations, for instance, that in Russia, the Rosfin monitoring agency has used its anti-money laundering efforts not to catch or discourage criminals but to target and attack the current regime's political enemies.

Another challenge for the FATF is the fact that bank secrecy rules are not homogenous around the globe. For example, until recently, it was a crime under Swiss law for a Swiss bank to reveal any information about an account holder, or the transactions associated with that account, absent strong evidence of a crime. (In Switzerland, tax avoidance is not a crime.) While Swiss banking law is evolving under global pressure, there is no organic rush for reform in Switzerland, where banking represents roughly 20 percent of the country's gross domestic product.

Because it is difficult (if not impossible) to define the scope of the global problem — that is, how much money is being laundered or moved around the world by terrorists, where the money is coming from and where it is heading — it is challenging to measure the success, failure or even the outcomes of any anti-money laundering effort and thereby to assign an ROI (return on investment) to anti-money laundering investments. Again, these accounts

should be viewed in the light of risk mitigation and their efficacy determined in large part by what doesn't happen — fines, reputational damage, remediation costs, lost business — not what does result.

In the face of all these complexities, difficulties and challenges — and the money launderers and terrorists who know the rules nearly as well as the banks do and are constantly changing tactics to get money in and out of the financial system — all financial institutions must employ ever-more rigorous measures to comply with sovereign and global regulations. But given limited resources and finite capabilities, these measures must be risk based. Resources should be deployed to areas that are most vulnerable. The more thorough the risk analysis is, the more effective the measures will be.

Ultimately, it is unrealistic to think that one firm or even one industry can take on the bad guys alone. The expectation that banks will man the front-line defenses against criminal activity is a presumption that financial institutions were neither created nor designed to satisfy. However, as long as governments and regulatory agencies continue to cast banks in that role, financial institutions have no choice but to play the part as best they can. That means continually improving the ways in which banks protect themselves and the world's financial system against money launderers, criminals, and individuals and groups that try to do business with (or on behalf of) sanctioned countries. One can only hope that the future will bring greater levels of cooperation between governments and the financial sector. In the end, that is the only way to begin to defund criminal interests, terrorists and others who seek to sabotage the world's financial systems and use them to further these villains' own anti-social self-interests. ■

Peter Brooke
peter.brooke@fticonsulting.com
Managing Director
Forensic & Litigation Consulting
FTI Consulting

Christine Moran
christine.moran@fticonsulting.com
Managing Director
Forensic & Litigation Consulting
FTI Consulting

For more information and an online version of this article, visit ftijournal.com.