Anti-Money Laundering, Anti-Terrorist Financing, and The Global Banking System Three Anomalies

Walter P. Loughlin, Partner, K&L Gates LLP

Abstract

Any broadly implemented system of laws and regulations can lead to anomalies, unintended consequences, and departures from expected norms. This paper identifies three such anomalous circumstances arising from the requirements imposed on banks by the procedural regime designed to address the risks of money laundering and terrorist financing, and proposes how they may be modified to align more closely to the goals of the anti-money laundering and anti-terrorist financing legal regime.

Introduction

It has become commonplace to regard the anti-money laundering laws and regulations imposed on banks as an important weapon in the campaign against terrorist financing. While terrorist exploitation of the international banking system is well-known, and the elements of the anti-money laundering and anti-terrorist financing regime are familiar, this article focuses on three issues which can fairly be characterized as anomalous consequences of the development, implementation, and expansion of anti-money laundering and anti-terrorist financing laws and regulations.

- The reliance on a novel legal fiction to justify the seizure in the U.S. of funds deposited in non-U.S. banks.

- Claims against banks that they are liable for harm caused to persons injured or killed by terrorist violence on the ground that, even though the banks did not know their customers were using the banks to support terrorist groups, they *should have known* by virtue of their obligation to conduct due diligence on customers and to monitor account activity.

- The strict application of anti-money laundering and anti-terrorist financing regulations threatens to exclude from the banking and financial system legitimate businesses and individuals, especially low income and undocumented groups in developing and developed countries, thereby limiting unduly the scope of the legal and regulatory protections against money laundering and terrorist financing.

Definitions

At its core, money laundering refers to activities aimed at concealing or disguising the origins of the proceeds of crime. 18 U.S.C. § 1956(a)(2)(B)(i); *Cuellar v. United* States, 128 S.

Ct. 1994 (2008); *United States v. Santos*, 128 S. Ct. 2020 (2008).[1] Terrorism financing involves the raising and processing of funds to supply terrorists with resources to commit violence. According to the UN International Convention for the Suppression of Financing Terrorism, a person commits the crime of financing terrorism "if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense within the scope of the Convention, including conduct "intended to cause death or serious bodily injury to a civilian" who is not taking part in hostilities or armed conflict, with the purpose to "intimidate a population or to compel a government or an international organization to do or abstain from doing any act."[2]

In other words, while money laundering involves the concealment of the illicit origin of proceeds of crimes, terrorist financing is the collection or provision of funds for terrorist purposes. In the case of money laundering, the source of funds is always unlawful, such as from narcotics distribution or organized crime. In the case of terrorist financing, funds can be derived from both legal and illicit sources. The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the source of the money but to conceal the intended purpose of the funds.

Both money laundering and the financing of terrorism involve the illegitimate use of the financial sector. The strategies against terrorist financing and money laundering are the same—to attack the criminal or terrorist organization through its financial activities and to follow the paper or electronic trail to identify criminals or terrorists.

Essential Elements of Anti-Money Laundering and Anti-Terrorist Financing Procedures

The twin pillars of anti-money laundering and anti-terrorist financing regulations are customer due diligence ("know your customer") and account monitoring. To meet the "know your customer" and accounting monitoring requirements, a bank verifies the identity of the customer, understands the types of banking services the customer intends to use, monitors the customer's account for unusual patterns of transactions, and reports suspicious account activity to the relevant banking regulator.

These procedures have been part of U.S. law for over 40 years, at least since the 1970 passage of the Bank Secrecy Act. They were strengthened in the Patriot Act enacted by Congress following the September 11, 2001 attacks.[3] The U.S. law is consistent with

[1] The federal money laundering statute, 18 U.S.C. § 1956 *et seq.*, makes it a crime knowingly "to conduct …a financial transaction which… involves the proceeds of specified unlawful activity" with the intent "to conceal or disguise the nature, the location, the source, the ownership, or the control of such funds."

[2] The Convention, only a small portion of which is quoted *supra*, was adopted by the UN General Assembly in Resolution 54/105 on December 9, 1999. *See* www.un.org/law/cod/finterr.htm.

[3] The Bank Secrecy Act is codified at 31 U.S.C. § 5311, *et seq.* The regulations implementing the Bank Secrecy Act are set forth at 31 C.F.R. Part 103. *See generally*, W. Pagano, "Bank Secrecy Act Best Practices for Bank Customers to Follow," *The Metropolitan Corporate Counsel* 43 (October 2008).

international norms. The Financial Action Task Force, established in 1989 at the G-7 Summit Meeting in Paris, is comprised of 36 member jurisdictions. The Task Force has issued successive recommendations of legal, regulatory and operational standards for combating money laundering, terrorist financing, and other threats to and abuses of the international financial system, with the expectation that each member state will seek to make these standards part of its domestic law. *See, e.g.*, "International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations" (Feb. 2012), available at www.fatf-gafi.org.[4]

The "know your customer" and account monitoring process may be necessary but not sufficient to address the exploitation of the global banking system by terrorists. Consider the September 11 attacks. The FBI's investigation of the bank accounts of the 19 suspected September 11 terrorists led it to conclude that the entire operation cost $303,672. That amount would be very difficult to detect in a global banking system where many billions of dollars change hands every day—no matter how elaborate and effective an anti-terrorist financing system may be.[5]

The First Anomaly: The Seizure of Funds Deposited in the United States By Deeming Them to be Deposited in Foreign Bank Accounts

In 1977, Congress enacted the International Emergency Economic Powers Act, 50 U.S.C. § 1701-1706, which authorizes the President to impose sanctions in response to circumstances found to present an "unusual and extraordinary threat" to the national security, foreign policy, or the economy of the United States. Pursuant to this power, asset-blocking orders and other measures have been instituted against a number of countries, including Iran, Libya, Panama, Iraq, Cuba, and Sudan.[6] These executive orders have been limited in their reach to property within the United States. They typically refer to "all property and interests in property that are in the United States or that hereafter came within the United States, or that are or hereafter came within the possession or control of a United States person."[7] In short, such orders have no extra-territorial effect beyond the borders of the United States.

---

[4] For similar international norms, *see* International Monetary Fund, "Anti-Money Laundering and Combating the Financing of Terrorism - Report on the Review of the Effectiveness of the Program" (May 11, 2011), available at www.imf.org.

[5] The September 11 terrorists opened 24 checking accounts at four different banks in the United States. The average value of each account was between $3,000 and $4,000. *See* Cliff Stephens & Tom Crook, "Pressure From All Sides," *Bank Sys. & Tech.*, Oct. 7, 2002, available at http://banktech.com/story/BNK20021007500002; *see also* Paul Beckett, "Sept. 11 Attacks Cost $303,672, But Few Details of Plot Surface," *Wall St. J.*, May 15, 2002, at B4.

[6] For a more complete list of such executive orders, and other details, *see* M. Gruson, "The U.S. Jurisdiction Over Transfers of U.S. Dollars Between Foreigners and Over Ownership of U.S. Dollar Accounts in Foreign Banks," 2004 *Colum. B.L. Rev.* 721, notes 21-31 (2004).

[7] *Id.* at 4.

All of this changed with the events of September 11, 2001. On October 26, 2001, Congress enacted the Patriot Act, an acronym for Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.[8] Title III of the Patriot Act revised previous anti-money laundering statutes, strengthened the anti-money laundering and anti-terrorism regime in the United States, and for the first time, extended the seizure and forfeiture power to deposits held outside the United States in foreign banks. 18 U.S.C. § 981(k). Specifically, Section 319(a) of the Patriot Act, codified at 18 U.S.C. § 981k, authorizes the U.S. government to seize and forfeit funds from a foreign bank that has an interbank account in the United States. It provides, in pertinent part:

> "if funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States…the funds shall be deemed to have been deposited into the interbank account in the United States [and are subject to seizure and forfeiture]."9

This provision is premised on the legal fiction that money deposited in a foreign bank can be treated as having actually been deposited in a bank in the United States. The Patriot Act also broadened the government's forfeiture power to make clear that it is the mere deposit of forfeitable funds in a foreign bank—and not the continued presence of the funds in the foreign bank account at the time of the seizure—that triggers the forfeitability of funds in the U.S. bank where the foreign bank has a correspondent account. All the government need do to seize such funds is to establish probable cause that the funds deposited in the foreign account are linked to criminal activity. 18 U.S.C. § 981(b)(1)(2).

In theory, the U.S. bank where the funds are seized will debit the customer's account in the foreign bank, which then effectively converts the forfeiture of the U.S. funds into a forfeiture of the customer's funds. If this occurs as intended, there is no net loss for the U.S. bank. In reality, however, the foreign bank customer may have transferred the money to another branch, or to another bank altogether, leaving insufficient readily available funds to be debited. The ability of the foreign bank to trace the customer's account may also be limited if the funds are moved and held in another personal or business name.

The "deeming" of funds held abroad in a foreign bank to be funds deposited in a U.S. bank essentially amounts to the irrational proposition that "x" equals "not-x." This calls to mind the exchange between Alice and Humpty Dumpty on words and the power to determine their

[8] The Patriot Act received scant congressional deliberation. The legislation covered 350 different subject matters and 40 different government agencies. It is widely believed that few members of Congress read the 342-page Act. *See* E. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism," 55 *Baylor L. Rev.* 955, 972 (2003).

[9] Interbank accounts, also known as correspondent accounts, are used by foreign banks to offer services to their customers where the banks have no, or limited, presence. In view of the importance of U.S. currency and the U.S. market in the global economy, many foreign banks have interbank accounts in the United States through which many transactions flow. *See generally*, Minority Staff of S. Permanent Subcommittee on Investigation, 107th Cong., Report on Correspondent Banking: A Gateway for Money Laundering 11-14 (Comm. Print 2001).

meaning written 150 years ago by the Christ Church, Oxford, mathematics don, Charles Dodgson, better known as Lewis Carroll.

> Humpty Dumpty: "When I use a word, it means just what I choose it to mean—neither more nor less."
>
> Alice: "The question is whether you can make words mean so many different things."
>
> Humpty Dumpty: "The question is which is to be master—that's all."[10]

Within constitutional limits, Congress is the master of the definition of statutory text. Its assertion of power to seize and forfeit funds held abroad is clear, as the relevant House Report states, the goal is to "treat[ ] a deposit made into an account in a foreign bank that has a correspondent account at a U.S. bank as if the deposit had been made into the U.S. bank directly." H.R. Rep. No. 107-250(I), at 58 (2001). The only U.S. court to hear a challenge to these statutory provisions upheld them in their entirety. *United States v. Union Bank for Saving & Investment, Bank of New York, and Reuven Krauzer*, 487 F.3d 8 (1st Cir. 2007).

This statutory provision is a legal fiction, utilizing legerdemain to define foreign assets as domestic assets. A legal fiction has been described as "a proposition about…the legal system…which rests on factual premises known to be inaccurate at the time of the fiction's invocation." E. Moglen "Legal Fiction and Common Law Theory: Some Historical Reflections," 10 *Tel-Aviv Univ. Stud. in L.* 35 (1991). It was Jeremy Bentham, the 19th century English legal theorist and polymath, who once said that legal fictions "are to justice what swindling is to trade,"[11] and even went so far as to denounce the use of a legal fiction as "presumptive and conclusive evidence of moral turpitude."[12]

More important than this somewhat light-hearted digression about legal fictions and literary fantasies is the more serious concern, noted by some critics, that section 319(a) is inconsistent with traditional notions of territorial jurisdiction, a doctrine which "provides that each nation has the exclusive right to regulate the conduct of all residents, individuals, and corporations within its borders."[13] The Patriot Act provision takes no account of the country in which the foreign bank is located, that country's anti-terrorist financing laws and regulations, or the absence of any genuine link between the allegedly tainted funds abroad and the funds seized in the United States. Moreover, the statute prohibits the foreign bank from challenging the forfeiture by invoking the traditional defense that it is an innocent owner of the allegedly tainted funds. 18 U.S.C. § 981(k)(4)(B)(i). Under the statute, only the depositor can rely on the

---

[10] Lewis Carroll, *Through the Looking Glass* at 364 (1871).

[11] 7 Jeremy Bentham, *Works* 283 (Bowring ed. 1843).

[12] 9 *Id.* 77. No citation to the work of Jeremy Bentham would be complete without reference to the fact that, pursuant to the terms of his will, Mr. Bentham's taxidermied effigy is on display in a glass case in a non-descript corridor at University College, London. I am advised that on the occasion of significant university anniversaries, Mr. Benham is removed from the glass cabinet to join meetings of the College Council. The minutes of these meetings record Mr. Bentham as "present but not voting."

[13] Gruson, *supra*, note 3, at 761.

innocent owner defense even if the bank cannot debit the depositor's account to recoup the amount seized.

It is at least conceivable that one could believe that the importance of disrupting terrorist financing justifies new and unprecedented powers in order to facilitate the seizure of terrorist assets. That extraordinary circumstances require new and extraordinary powers is a familiar rationale. But a power once loosed, is difficult to cabin. The new seizure and forfeiture procedures are not being used exclusively, or even primarily, in connection with terrorist financing. The *Union Bank* case decided by the First Circuit involved a telemarketing fraud. Other cases subject to the Patriot Act procedures have involved the counterfeiting of luxury goods and internet sales of human growth hormone.

The Second Anomaly: Bank Liability for Terrorist Violence

The second anomaly of the anti-money laundering and anti-terrorist financing laws and regulations is that they are being used by plaintiffs in civil litigation against banks to argue (1) bank customers used the banks to finance terrorism, and (2) the banks must have known this by virtue of their obligation to "know their customers" and monitor account activity. In other words, the procedures banks have implemented to combat terrorist financing are now being turned against them as a basis for claims that the banks have legal liability for the very terrorist violence they have sought to prevent and detect. Irony is too mild a word to describe these circumstances.

The civil litigation in which these and similar claims are being made involves plaintiffs who have been injured in terrorist violence and the relatives of persons who were killed by such violence. Lawsuits have been commenced in U.S. courts against a large number of banks, including: Credit Lyonnais, UBS, Nat West, Bank of China, American Express Bank, and Lebanese-Canadian Bank (formerly a division of Royal Bank of Canada). Many of these cases were initiated by an Israeli organization called Shurat HaDin and its cooperating lawyers. The Shurat HaDin website proclaims its mission to be "to bankrupt the terror groups and grind their criminal activities to a halt—one lawsuit at a time."[14] It may be more accurate to describe the mission as imposing such heavy costs on banks that are alleged to have customers using bank facilities to aid terrorist groups such that, over time, the banks will take steps to limit or deny access to such customers to the global banking system.[15]

[14] www.israellawcenter.org

[15] One major weapon in the anti-terrorist financing arsenal is the list of "Specially Designated Nationals" ("SDN") maintained by the U.S. Treasury Department's Office of Foreign Asset Control, which includes persons suspected of terrorism. *See* www.treasury-gov/ofac/about/organizational-structure.gov. Many banks have installed software which includes the OFAC list in order to detect and interdict terrorist use of bank facilities. One consequence of this process is that a bank may begin to overly rely on the list and believe that a bank customer whose name is not the SDN list involves no risk of terrorist use of the bank's facilities.

In each of these cases, it is alleged that the banks had customers who used banking facilities, such as wire transfers, to support terrorist groups who later committed violent acts that injured or killed a plaintiff or a plaintiff's relative. The focus of this article is the intersection of the allegations of the bank's knowledge and its anti-money laundering and anti-terrorist financing procedures. If it could be proved that a bank has actual knowledge, *i.e.*, knowingly assisted an agent of a terrorist group to funnel money to that group, it would be consistent with settled legal principles and elemental fairness to hold the bank at least partly responsible for injuries or deaths subsequently caused by that group. But the allegations of the banks' knowledge in these lawsuits are a far cry from any claim that they had actual knowledge of any link between their customers and terrorism.

One example is illustrative of the wave of current litigation and therefore will suffice. In 2009, over fifty Israeli citizens, victims themselves or relatives of victims injured or killed in rocket attacks or bombings in Israel committed by Hamas or Palestine Islamic Jihad, sued the Bank of China ("BOC") in New York State Supreme Court. The Complaint alleges that a single BOC customer at a single branch in Guangzho—one of the 10,000 such branches in China, was "a senior operative and agent of Hamas and Palestine Islamic Jihad." The lawsuit's damage claim is for $750 million.

Among its knowledge allegations, the Complaint contends that the Guangzho branch "should have known" that the customer was using the branch's wire transfer facilities "for illegal purposes" because of BOC's duties, *inter alia,* under United States law and the Financial Action Task Force rules "to know their customers, perform due diligence, and not provide banking services to customers who act in a suspicious and/or irregular manner…".[16]

The Complaint also alleges that there was activity in the customer's account that would be "universally recognized by all professional bankers, including Defendant BOC and its employees, as typical indicia of transactions made for illegal purposes." Therefore, BOC "should have known that the customer was using the branch's wire transfer facilities for illegal purposes." The account activity which purportedly gave rise to this knowledge is alleged to be as follows:

- Most of the wire transfers were made in cash;
- Most of the money sent by wire transfer was withdrawn on the same day it had been received or on the following day.
- The sums involved were large, mostly in the range of $100,000 or more;

[16] *Elmaliach, et al. v. Bank of China Limited*, Index No. 102026/07 (N.Y. Sup. Ct.). *See also Rothstein v. UBS AG*, 08 Civ. 4414 (S.D.N.Y.); *Licci v. American Express Bank Ltd. and Lebanese Canadian Bank*, SAL, 08 Civ. 7253 (S.D.N.Y.). Many of these cases also allege that the bank actually knew that its customer was a terrorist and knew the bank was being used to finance terrorism. To date, no evidence of such actual knowledge has been produced in these cases.

- The intervals between transfers were often short (weeks or days) and the sums transferred were often identical or similar. For example, many of the transfers were for $99,960, $99,970 or $99,990;

- Many of the transfers were for round figures;

- Many of the transfers were structured to be slightly less than round figures. For example, many of the transfers were for $99,960, $99,970, $99,990 or $199,965.

My purpose here is not to argue the merits of these claims, although I cannot help but observe the contradictory nature of the description of wire transfers that were in round figures except when they were in less than round figures, and that the transfers were more than $100,000 except when they were less than $100,000. Even if this account activity could be regarded as suspicious, triggering a report to BOC's regulator, it would not necessarily be indicative of terrorist financing.[17]

The Complaint's knowledge allegation is based on the concept known as constructive, rather than actual, knowledge. Constructive knowledge has been defined as knowledge that a person will be legally presumed to have—even in the absence of actual knowledge—as long as a reasonably diligent person would or could have gained that knowledge. *Merck Co. v. Reynolds*, 2010 U.S. LEXIS 3671 (2010) (a person will be charged with actual knowledge of a fact if a hypothetical reasonably diligent person could have learned the fact); *Berman v. Keagan & Co.*, 2011 WL 1002683 at *10 (S.D.N.Y. March 14 2011) (constructive knowledge is "knowledge that one using reasonable care or diligence should have, and is attributed by law to a given person.")

The outcome of these cases will not be known for years to come.[18] What is clear even now, however, is that the banks have incurred massive expenses defending these cases and litigating the alternative claims related to their actual or constructive knowledge—to say nothing of the substantial reputational damage they have experienced in being accused publicly of

[17] In the interest of full disclosure, I should acknowledge that I represented the Bank of China in this case and several others like it for three years. I am no longer involved in the cases. Based on my personal knowledge of the case, the BOC branch in Guangzhou did know its customer. Bank officers knew him to be from Gaza and to have a Palestinian passport, a copy of which was in their files. They also knew the customer to be operating a children's clothing store, which they had visited. Guangzhou is the third most populous city in China, after Beijing and Shanghai, and is within a special economic zone with robust economic activity involving people and businesses from every corner of the world.

[18] The cases against two banks, UBS and American Express Bank, have been dismissed. In *Rothstein v. UBS*, 08 Civ. 4414 (JSR), which involved forty-five victims or families of victims of terrorist violence committed by Hamas or Hezbollah, the Court found the pleading of the bank's causal responsibility for the terrorist violence legally insufficient. In *Licci v. American Express Bank, Ltd.*, 704 F. Supp. 2d 403 (S.D.N.Y. 2010), the Court dismissed the Complaint on the ground that the allegation of the bank's knowledge was unsupported by sufficient factual allegations. Appellate review of these dismissals has been sought. On March 5, 2012, the United States Court of Appeals for the Second Circuit affirmed the district court's dismissal of the Complaint against American Express Bank. *Licci v. American Express Bank, Ltd.*, Dkt. No. 10-1306-cv (2d Cir. March 5, 2012).

supporting terrorist financing and contributing to terrorist violence. These circumstances can lead one to ponder whether the banks have had occasion to feel a twinge of regret that they so actively took on board anti-money laundering and anti-terrorist financing procedures only to see those procedures used against them in litigation claims to the effect that the banks are liable for the very terrorist violence they sought to prevent and detect.

The Third Anomaly: The Paradox of Exclusion from the Financial System

More than one-half of the world's adult population lacks access to credit, insurance, savings accounts, and other formal financial services. The number of adults without access to banking institutions is estimated to be 2.7 billion (72% of adults) in developing countries and 160 million (19% of adults) in developed countries. In 2010, more than 215 million people (or 3% of the world's population) lived outside their countries of birth and sent an estimated $325 billion to developing countries.[19] The terms "unbanked," "underbanked," and "underserved" are used to describe persons with restricted or no access to banks or wider financial services.

There are, of course, many reasons why people may be excluded from the financial system that have nothing to do with anti-money laundering and anti-terrorist financing procedures, including cultural mistrust of mainstream financial institutions as safe repositories of money, language barriers, or issues of proximity to financial services. For many people in different parts of the world, opening a bank account, receiving a loan, withdrawing money or making a payment requires going to a bank branch, ATM, or point-of-sale terminal. Such access points to the financial system may be extremely limited in developing countries.

Nonetheless, there is a growing recognition that anti-money laundering and anti-terrorist financing procedures are contributing to the exclusion of people from the financial system. This has led to calls for greater flexibility in the application of the twin pillars of these procedures—customer due diligence and account monitoring. The calls for reform coalesce around the notion of a more risk-based approach to these regulations that takes into account (1) alternative but acceptable means for accomplishing customer due diligence and (2) distinguishing between accounts that have small balances and need less monitoring and larger accounts with greater activity which call for a higher level of monitoring.

Customer Due Diligence

There are many countries where a broader range of identification documentation is becoming acceptable. In India, for instance, a person who is not able to produce formal identification

[19] *See* Consultative Group to Assist the Poor (CGAP), *Financial Access 2009: Measuring Access to Financial Services Around the World*, available at www.cgap.org/gm/document-1.9.38735/FA2009.pdf; *see also* World Bank, *Poverty Reduction and Equity*, available at web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTPOVERTY/0,,contentMDK:22569498~pagePK:148956~piPK:216618~theSitePK:336992,00.html; World Bank, *Migration and Remittances*, available at web.worldbank.org/WBSITE/EXTERNAL/TOPICS/0..contentMDK:21924020~pagePK:5105988~piPK:360975~theSitePK:214971,00.html.

documents may be able to open an account if a current bank customer, who has been subject to the full due diligence and whose account has been satisfactorily monitored for at least six months, introduces the new customer to the bank and certifies to the accuracy of the new customer's photograph and address. In rural areas of the Philippines, a certificate issued by the head of a village is acceptable proof of identification and residence. In Malaysia, some individuals have no fixed residential address, especially in rural areas. Banks there will accept a postal address, which is often a communal post box, or a neighbor's address. In Fiji, acceptable identification and residence information can be furnished by village headmen, religious leaders, and current or former employers.[20] In future, technological change may address this issue on a broader scale. Indonesia and other Asian countries are developing smart cards to be used as a form of universal identification.[21]

Risk-Based Account Monitoring

As the financial system becomes more inclusive, the burden on banks to apply full anti-money laundering and anti-terrorist financing monitoring equally to all accounts has also come into question. A report issued by the Financial Action Task Force last year encouraged member states to experiment with a more risk-based approach to account monitoring. Specifically, the Task Force proposed the following recommendation:

> When a financial activity is carried out by a natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is a low risk of money laundering or terrorist financing, a country may decide that the application of AML/CFT measures is not necessary, either fully or partially.[22]

France is one of the first countries to experiment with this approach. It has identified two types of business—currency exchange and insurance intermediaries—where it believes the risk of money laundering and terrorist financing is low and therefore more proportionate regulatory intensity is appropriate. However, mindful of the importance of the risk-based approach, France will reduce the regulatory scrutiny of the activity of these businesses only if no single transaction exceeds EUR 1,000 and annual total transactions do not exceed EUR 50,000.[23]

In India, migrant laborers are allowed to open small accounts where the balance of such accounts cannot exceed 50,000 rupees (approximately $1,000) and no monthly withdrawal or transfer can exceed 10,000 rupees (approximately $200).[24] As long as the accounts are maintained at these levels, they present no risk of money laundering or terrorist financing and require no active monitoring.

---

[20] *See generally* Financial Action Task Force, *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (June 2011).
[21] *Id.* at 29, note 43.
[22] *Id.* at 20.
[23] *Id.* at 22.
[24] *Id.* at 33.

Not only are these new steps toward financial inclusion desirable in their own right, they also, perhaps paradoxically, can be viewed as simultaneously relaxing and strengthening the anti-money laundering and anti-terrorist financing regime. This is so because persons excluded from the financial system often resort to what is available in the informal, unregulated, undocumented, and largely cash economy. There are, of course, anti-money laundering and anti-terrorist financing risks in the underground economy that can compromise the ability of the regulatory system to prevent and detect such risks. Seen from this perspective, financial inclusion—the movement of more financial transactions into the formal banking and financial system—will facilitate the detection and prevention of the wrongful use of the financial sector through the use of a more flexible and risk-based approach to money laundering and terrorist financing procedures.

Conclusion

It is perhaps a truism that broadly implemented legal and regulatory systems imposed on dynamic institutions, such as the international financial sector, are bound to give rise to unintended results and anomalous consequences. New circumstances can prompt novel applications of familiar procedures. In order for any such legal and regulatory scheme to maintain its vitality, it must be adaptable to unanticipated issues and circumstances. The flexibility that is occurring in customer due diligence and account maintaining procedures in reaction to the lack of access to the banking system in many parts of the developing and developed world are hopeful signs.

However, the other two anomalies discussed in this article are more worrisome. Both threaten to undermine commitment to anti-terrorist and anti-money laundering efforts. The litigation campaign to hold banks liable for terrorist violence, and to use the "know your customer" and account monitoring procedures to argue that the banks "should have known" of alleged terrorist use of bank facilities, could cause banks to question the cost-benefit ratio of implementing such procedures. The use of the concept of constructive knowledge to impute knowledge of a bank's participation in terrorist violence risks injustice. None of these cases should lead to bank liability in the absence of sufficient proof of actual knowledge.

The unilateral seizure of funds in U.S. banks that are "deemed" to be tainted funds held in foreign banks risks alienating foreign banks and compromising the sharing of information and common effort to address terrorist financing that is needed to strengthen globally the legal and regulatory regime. I propose the following recommendations.

First, the new seizure and forfeiture powers should be limited to circumstances involving terrorist financing rather than ordinary criminal offenses. Congress created this new, more potent, set of powers in order to address terrorist financing. These provisions should be confined to their legislative rationale.

Second, U.S. authorities should distinguish between countries that have a comprehensive set of procedures to address terrorist financing and those that do not. If a country has the full complement of anti-terrorist financing laws and regulations, there should be little need to invoke the new Patriot Act provisions. If a country has no such laws, regulations, and procedures—or has proved itself incapable or unwilling to enforce them—the U.S. Federal Reserve can and should take steps to prevent foreign banks from any such countries from having correspondent accounts at U.S. banks, a measure that is a more proportionate approach than reliance on the fiction that foreign bank deposits are deemed to be deposited in a U.S. bank.

Published by the Forum on Public Policy