The Extraterritorial Reach of U.S. Anti-Terrorist Finance Laws

Criminal prosecution and civil litigation risk for non-U.S. financial institutions arising from operations outside the United States

Table of Contents

I. Introduction and Background
1. Scope of Article
2. What is Terrorist Financing?
3. Overview of the U.S. Post-9/11 Response to Terrorist Financing

II. U.S. Anti-terrorist Finance Laws with Global Reach
1. OFAC Sanctions
   1.1 Potential Extraterritorial Effects for Non-U.S. Financial Institutions
   1.2 Case Study: Lloyds TSB Bank plc
   1.3 Questions to Help Identify Potential OFAC Exposure to Non-U.S. Financial Institutions
2. The Anti-Terrorism Act
   2.1 Potential Extraterritorial Effects for Non-U.S. Financial Institutions
   2.2 Case Study: NatWest
   2.3 Questions to Help Identify Potential ATA Exposure to Non-U.S. Financial Institutions
3. The Alien Tort Statute
   3.1 Potential Extraterritorial Effects for Non-U.S. Financial Institutions
   3.2 Case Study: Arab Bank PLC
   3.3 Questions to Help Identify Potential ATS Exposure to Non-U.S. Financial Institutions

III. Conclusion

I. Introduction and Background

1. Scope of Article

Increasingly U.S. statutes and regulations designed to combat global terrorist financing are being interpreted and prosecuted expansively, creating potential criminal and civil exposure for non-U.S. financial institutions based on conduct occurring wholly or largely outside of the United States. Non-U.S. institutions ignore this trend at their own peril. For example:

- In January 2009, Lloyds TSB Bank plc agreed to pay fines of $350 million to the U.S. Government and the State of New York based on allegations that its non-U.S. offices had cleared dollar transactions through U.S. correspondent banks largely on behalf of Iranian banks, in violation of U.S. sanctions against Iran – a country the U.S. has sanctioned due to, among other things, Iran's support for international terrorism and active pursuit of weapons of mass destruction ("WMDs").

- In 2005, primarily U.S. victims of Hamas terrorist attacks in Israel sued National Westminster Bank PLC ("NatWest") in federal court in New York, seeking to hold NatWest liable for treble damages under the Anti-Terrorism Act ("ATA") based on allegations that NatWest violated the ATA by maintaining a non-dollar account in London for an alleged Hamas front, Interpal, notwithstanding the fact that U.K. authorities had frozen, investigated, and subsequently unfroze Interpal’s account after finding no "pro-terrorist" bias in Interpal’s prior distributions of funds.

- Despite the absence of any U.S. conduct by the banks, non-U.S. victims of Hamas and Hezbollah terrorism sued non-U.S. banks in U.S. courts under the Alien Tort Statute ("ATS"), in some cases seeking damages of over $500 million, based on allegations that the banks maintained accounts for and/or processed funds transfers received by alleged terrorist front organizations in Europe and the Middle East.

This article is intended to provide financial institutions, particularly those headquartered outside of the United States, with a basic understanding of the risks arising from extraterritorial application of U.S. anti-terrorist financing laws and provides some thoughts on how to identify such risks.

The article begins with a brief overview of what terrorist financing is and how the United States has sought to curtail it. It then discusses in more detail, and with illustrative examples, several important U.S. laws – i.e., U.S. economic sanctions, the ATA, and the ATS – that may give rise to criminal and/or civil liability in cases involving terrorist financing against non-U.S. financial institutions.
institutions based on conduct occurring largely, if not exclusively, outside of the United States. For each law discussed, this article provides some guidance to help non-U.S. financial institutions determine whether they are involved in the type of business activity that may give rise to the particular risk at issue.

2. What is Terrorist Financing?

The 1999 United Nations International Convention for Suppression of the Financing of Terrorism (the «Financing Convention») prohibits terrorist financing. A person commits an offense under article 2 of the Financing Convention 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» either acts intended to kill or seriously injure civilians, or certain other enumerated acts of terrorism as defined in other international conventions, such as the 1997 International Convention for the Suppression of Terrorist Bombings.\(^1\) The Financing Convention is not self-executing; that is, member states must enact their own implementing legislation in order to provide a domestic mechanism for the prosecution and punishment of conduct prohibited by the Financing Convention.\(^2\) Accordingly, the Financial Action Task Force\(^3\) (the «FATF»), an intergovernmental body that, among other things, develops and promotes policies to combat terrorist financing, urges countries to ratify the Financing Convention and to enact domestic legislation to implement it.\(^4\) A number of countries—including the United States\(^5\)—have done so. Such domestic statutes often enact verbatim the language prohibiting terrorist financing in Article 2 of the Financing Convention.\(^6\) Therefore, the key language from the Financing Convention, making it unlawful to «provide or collect funds» to support acts of terrorism, appears in a number of domestic statutes.\(^7\)

Although Article 2 of the Financing Convention prohibits «provide\(\)ing\(\)» and «collect\(\)ing\(\)» funds to carry out acts of terrorism, the Financing Convention does not define the terms «provide» and «collect.» However, the Convention’s drafters most likely meant for the Financing Convention to address two distinct evils: (1) donating gifts or funds or assets to terrorists, and (2) engaging in fundraising on behalf of terrorists.\(^8\) These twin concerns are crucial to the U.S. anti-terrorism agenda. The 2004 staff report to the National Commission on Terrorist Attacks Upon the United States (the «9/11 Commission»), for example, explains that «[t]he term ‘terrorist financing’ is commonly used to describe two distinct types of activity. First, it can consist of the financing of operational terrorist cells, like the 19 hijackers who conducted the 9/11 attacks. This financing consists of the funds the cell needs to live and to plan, train for, and commit the terrorist act. The second type of terrorist financing is fundraising — the process by which an organized terrorist group, such as al Qaeda or Hamas, raises money to fund its activities. Such fundraising often takes place through nongovernmental organizations, which may raise money for legitimate humanitarian purposes and divert a fraction of their total funds for illicit purposes.»\(^9\)

3. Overview of the U.S. Post-9/11 Response to Terrorist Financing

In the wake of 9/11, the United States (like many other nations in the international community) has employed a multi-faceted strategy for combating terrorist financing that emphasizes, among other things: (1) freezing the assets, both domestically and internationally, of terrorists, their front companies and their active supporters; (2) implementing regulatory measures to prevent terrorists from using the financial system to facilitate terrorist financing; (3) developing international standards to prevent the financing of terrorism; (4) prosecuting criminal actions against terrorist financiers and their front entities; and (5) providing for private civil causes

---

2 Financing Convention, supra note 1, arts. 4–9.
3 FATF/GAFI, http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html (last visited July 12, 2009).
4 Mark Pieth, Criminalizing the Financing of Terrorism, 4 J. Internat’l Crim. Just.1274, 1275 (Nov. 2006) («Pieth») («Among the most prominent requirements of the FATF Special Recommendations on Terrorist Financing is the recommendation to ratify and implement the [Financing Convention]»).
7 See, e.g., Article 260quinties of the Swiss Penal Code («Wer [...] Vermögenswerte sammelt oder zur Verfügung stellt»).
of actions against those who provide financial support intended to foster terrorism. To achieve these goals, the United States has, in conjunction with other initiatives, enacted a substantial body of post-9/11 laws and regulations that define new crimes, create new criminal causes of action, expand the jurisdictional reach of U.S. laws, and enhance the authority of U.S. prosecutors to target, investigate, and prosecute domestic and foreign individuals, financial institutions, and other entities. In many instances, the U.S. courts have read these new laws (as well as certain older, pre-9/11 laws) expansively in cases concerning terrorist financing, thereby broadening the extraterritorial reach of U.S. law and expanding the exercise of U.S. jurisdiction in such cases.

In contrast, prior to 9/11, anti-money laundering legislation provided the primary weapon in the U.S. statutory arsenal in the fight against terrorist financing. But money laundering laws were not well suited for that task in several respects, including that such laws were outmoded, because money laundering occurs only with the proceeds of criminal activity, whereas terrorist financing often occurs with funds that are lawfully obtained (and then subsequently used for an unlawful purpose), and that because terrorist financing can involve relatively small amounts that would not otherwise be detected through traditional means of detecting money laundering, such as currency transaction reports («CTRs») or suspicious activity reports («SARs»). Also, there is no private right of action under the U.S. anti-money laundering statutes.

Given the perceived need for more robust anti-terrorist financing measures, the U.S. Legislative and Executive Branches took action to enhance the government’s tools for disrupting terrorist financial networks. Measures taken that are most relevant for financial institutions include, among others, the following:

- On September 23, 2001, acting under the authority of the International Emergency Economics Powers Act (the «IEEPA»), President Bush issued Executive Order 13224. The Order blocks the assets of terrorists and their affiliates that are identified on a list compiled by U.S. authorities. The Executive Order also blocks the assets of any other persons or entities that the Executive Branch identifies as assisting or sponsoring terrorism, including those persons or entities that «provide financial, material or technological support for, or financial or other services to, or in support of . . . acts of terrorism.» A U.S. Treasury Department Fact Sheet describes the foregoing provision as «establish[ing] our ability to block the U.S. assets of, and deny access to U.S. markets to, those foreign banks that refuse to freeze terrorist assets.» The Executive Order requires the U.S. Treasury and State Departments to develop a list of persons or entities whose assets will be subject to blocking under the Order, including persons or entities who have committed or pose a significant risk of committing terrorist acts, or who finance terrorists or acts of terrorism, or who provide financial or other services to terrorists. The individuals or entities that are listed are labeled «Specially Designated Global Terrorists» («SDGTs»). The requirement to block (i.e., to freeze) SDGT assets generally applies to all SDGT assets in the territory or possession of the United States. The Executive Order does not require that a person or entity know, or intend, that their conduct will assist terrorists or an act of terrorism in order for that person or entity to be listed and its assets subject to blocking.

- On October 26, 2001, the United States enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the «USA PATRIOT Act»). Title III of the USA PATRIOT Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. Therein, Congress found that «money laundering, and the defects in financial transparency on which money launderers rely, are critical to the financing of global terrorism and the provision of funds for terrorist attacks.» Accordingly, Title III implemented new provisions designed «to increase the strength of Uni-

12 Executive Order 13224, §§ 1(b), 1(d)(i).
13 Id. § 302(a)(2).
16 Id. § 302(a)(2).
18 Id. § 302(a)(2).
As the discussion and case studies set forth below illustrate, it is essential for non-U.S. financial institutions to understand the broad, often extraterritorial reach of U.S. laws in the field of anti-terrorist financing, to better identify and mitigate the risk of potential administrative, civil and criminal liability in the United States.

On June 25, 2002, the United States enacted the Suppression of the Financing of Terrorism Convention Implementation Act of 2002, which amended an existing domestic law – the ATA – to add provisions implementing the Financing Convention by making it a crime to provide or collect funds with the intention that the money be used for terrorist activities. The ATA also makes it unlawful to knowingly provide material support (including financial services) or resources to an organization designated by the United States as a Foreign Terrorist Organization («FTO»). Under Section 219 of the Immigration and Nationality Act, the Secretary of State, in consultation with the Attorney General and the Treasury Department, may designate a foreign entity as an FTO if it engages in terrorism, or retains the intent and capacity to engage in terrorism. In addition, the ATA provides a private federal civil cause of action, under which U.S. persons injured by an act of international terrorism may recover treble damages and attorneys’ fees.

As the ATA came into effect, OFAC expanded its role to coordinate with other U.S. agencies and instrumentalities and in some cases, their nationals wherever located (e.g., Cuba) and, in some cases, with individuals located in the sanctioned countries (e.g., persons in Iran).

In addition to prohibiting business activities with certain countries, OFAC implements list-based sanctions that prohibit business dealings with Specially Designated Nationals («SDNs»). SDNs include persons or entities listed for any of a variety of reasons, including those listed due to terrorism concerns, such as SDGTs and FTOs, discussed above. The SDN List and a summary of the various sanctions programs implemented by OFAC can be found on the OFAC website.

Sanctions implemented by OFAC generally are binding on «U.S. persons» – «U.S. persons» include U.S. citizens and residents, wherever located, entities organized under the laws of the United States and their foreign branches, and any person located in the United States including U.S. branches of non-U.S. banks. For cer-

II. U.S. Anti-terrorist Finance Laws with Global Reach

1. OFAC Sanctions

The Office of Foreign Assets Control («OFAC») of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries and regimes, terrorists and other threats to the national security, foreign policy or economy of the United States. Once individuals, groups, or entities are designated by the Treasury or the State Department, OFAC is responsible for prohibiting transactions with them and, where applicable, enforcing the blocking (i.e. freezing) of assets subject to U.S. jurisdiction or, in certain circumstances, granting licenses to permit certain transactions that would otherwise be prohibited.

Country-based sanctions generally bar unlicensed business activities with specified countries as well as with their agencies and instrumentalities and in some cases, their nationals wherever located (e.g., Cuba) and, in some cases, with individuals located in the sanctioned countries (e.g., persons in Iran).

Sanctions implemented by OFAC generally are binding on «U.S. persons» – «U.S. persons» include U.S. citizens and residents, wherever located, entities organized under the laws of the United States and their foreign branches, and any person located in the United States including U.S. branches of non-U.S. banks. For cer-

27 Terrorist Financing, supra note 8, at 18 («OFAC . . . coordinates and works with other U.S. agencies to identify and investigate prospective terrorist designations; . . . compiles the administrative record or evidentiary material that will serve as the factual basis underlying a decision by OFAC to designate individuals or groups; and . . . engages foreign counterparties to gather information, apply pressure, or request or offer assistance in support of terrorist designation and asset blocking activities»).
30 The regulations implementing each sanctions program contain a definition of U.S. person or person subject to the jurisdiction of the United States. See, e.g., 31 C.F.R. § 588.315 (Sudanese Sanc-

19 For example, among other provisions, Section 319 of the USA PATRIOT Act, allows a U.S. prosecutor to initiate U.S. court proceedings to obtain the attachment and forfeiture of assets in a non-U.S. bank’s U.S. correspondent account, based on allegations that one of the bank’s customers deposited an equivalent amount of assets, obtained in violation of U.S. law, with the bank somewhere, including outside of the United States. Under Section 319, attachment and forfeiture are possible even though the assets in the bank’s U.S. correspondent account may have no relation to the particular customer who violated U.S. law, or to the illegally obtained assets. Moreover, unless the bank has discharged its obligation to its customer, it is the customer, and not the bank, that is the «owner» of the seized funds, eligible to challenge the forfeiture on the grounds of innocence or other defenses.

20 Id. § 302(b)(i).
23 18 U.S.C. § 2393C.
24 Id. § 2393B.
1.1 Potential Extraterritorial Effects for Non-U.S. Financial Institutions

There are several ways in which OFAC sanctions laws may have extraterritorial reach.

First, as noted above, U.S. citizens and residents, wherever located (e.g., expatriate employees, visiting staff members, contractors performing services in non-U.S. offices), generally must comply with U.S. sanctions laws.

Second, under IEEPA it is unlawful to «violate, attempt to violate, conspire to violate, or cause a violation» of any regulation or prohibition issued under the IEEPA, i.e., to violate OFAC regulations such as the Iran sanctions discussed above. The phrase «cause a violation,» added to IEEPA in 2007, applies to conduct in which a party not directly covered by OFAC regulations causes a party that is covered by OFAC regulations (e.g., non-U.S. banks or banks outside of the United States) unwittingly to violate those regulations, as may arguably occur if a foreign financial institution not directly covered by OFAC regulations engages in conduct that causes its U.S. correspondent bank to violate OFAC prohibitions without knowing that it is doing so.

1.2 Case Study: Lloyds TSB Bank plc

On January 9, 2009, the United States Department of Justice («DOJ») filed in federal court in Washington, D.C., a one-count criminal information against Lloyds TSB Bank plc («Lloyds») for violation of the IEEPA, alleging that Lloyds knowingly and willfully violated the prohibitions against exporting services, including financial services, from the United States to Iran. Simultaneously, the DOJ announced that it had entered into a Deferred Prosecution Agreement (DPA) with Lloyds. The Office of the District Attorney for the County of New York, which coordinated with the DOJ on the Lloyds investigation, at the same time announced that it had entered into a parallel Deferred Prosecution Agreement with Lloyds (this article refers to the two agreements collectively as the «DPA»).

On October 25, 2007, the property and interests of two Iranian financial institutions (Bank Mellat and Bank Melli) were blocked under OFAC sanctions with respect to WMD proliferation and another (Bank Sederat) was blocked for support to terrorist organizations. On January 9, 2007, another Iranian financial institution (Bank Sepah) also was blocked due to WMD concerns. See Recent OFAC Actions, Nov. 20, 2007, available at http://www.treas.gov/offices/enforcement/ofac/actions/20071120.shtml.

50 U.S.C. § 1705(s).
51 On October 25, 2007, the property and interests of two Iranian financial institutions (Bank Mellat and Bank Melli) were blocked under OFAC sanctions with respect to WMD proliferation and another (Bank Sederat) was blocked for support to terrorist organizations. On January 9, 2007, another Iranian financial institution (Bank Sepah) also was blocked due to WMD concerns. See Recent OFAC Actions, Nov. 20, 2007, available at http://www.treas.gov/offices/enforcement/ofac/actions/20071120.shtml.

Penalties for noncompliance with sanctions laws may include fines and, if noncompliance is willful, imprisonment. IEEPA provides for civil liability for violations of U.S. sanctions laws on a strict liability basis. This means that even if a party subject to U.S. sanctions laws does not know that its conduct is violating those laws, it still may be held liable. As a practical matter, however, OFAC generally does not pursue enforcement actions against parties that unwittingly engage in transactions with or on behalf of sanctioned parties.

Second, under IEEPA it is unlawful to «violate, attempt to violate, conspire to violate, or cause a violation» of any regulation or prohibition issued under the IEEPA, i.e., to violate OFAC regulations such as the Iran sanctions discussed above. The phrase «cause a violation,» added to IEEPA in 2007, applies to conduct in which a party not directly covered by OFAC regulations causes a party that is covered by OFAC regulations (e.g., non-U.S. banks or banks outside of the United States) unwittingly to violate those regulations, as may arguably occur if a foreign financial institution not directly covered by OFAC regulations engages in conduct that causes its U.S. correspondent bank to violate OFAC prohibitions without knowing that it is doing so.

1.2 Case Study: Lloyds TSB Bank plc

On January 9, 2009, the United States Department of Justice («DOJ») filed in federal court in Washington, D.C., a one-count criminal information against Lloyds TSB Bank plc («Lloyds») for violation of the IEEPA, alleging that Lloyds knowingly and willfully violated the prohibitions against exporting services, including financial services, from the United States to Iran. Simultaneously, the DOJ announced that it had entered into a Deferred Prosecution Agreement (DPA) with Lloyds. The Office of the District Attorney for the County of New York, which coordinated with the DOJ on the Lloyds investigation, at the same time announced that it had entered into a parallel Deferred Prosecution Agreement with Lloyds (this article refers to the two agreements collectively as the «DPA»).

On October 25, 2007, the property and interests of two Iranian financial institutions (Bank Mellat and Bank Melli) were blocked under OFAC sanctions with respect to WMD proliferation and another (Bank Sederat) was blocked for support to terrorist organizations. On January 9, 2007, another Iranian financial institution (Bank Sepah) also was blocked due to WMD concerns. See Recent OFAC Actions, Nov. 20, 2007, available at http://www.treas.gov/offices/enforcement/ofac/actions/20071120.shtml.

50 U.S.C. § 1705(s).
51 On October 25, 2007, the property and interests of two Iranian financial institutions (Bank Mellat and Bank Melli) were blocked under OFAC sanctions with respect to WMD proliferation and another (Bank Sederat) was blocked for support to terrorist organizations. On January 9, 2007, another Iranian financial institution (Bank Sepah) also was blocked due to WMD concerns. See Recent OFAC Actions, Nov. 20, 2007, available at http://www.treas.gov/offices/enforcement/ofac/actions/20071120.shtml.
In sum, pursuant to the DPA, Lloyds agreed to forfeit $350 million ($175 to the United States, $175 million to New York County), which prosecutors said represented the value of wire transfers that Lloyds cleared through its U.S. correspondent accounts between 2002 and 2007 after having first deliberately removed from its funds transfer messages (i.e., SWIFT messages) certain information about the parties and/or banks involved in the transactions. According to the facts to which Lloyds agreed, Lloyds’ actions prevented the automated systems that its U.S. correspondent banks use to screen transactions for OFAC compliance («OFAC filters») from detecting transactions that otherwise would have been stopped, investigated, and subsequently blocked or rejected by the U.S. correspondent banks in accordance with OFAC sanctions against Iran, Sudan and (prior to September 2004) Libya.37

The New York County District Attorney’s press release explains:38

New York banks use sophisticated computer systems to monitor and screen all wire transfer activities to ensure that the banks do not engage in prohibited transactions. The banks depend on these automated systems to prevent sanctioned entities from accessing the United States banking system. The investigation revealed that LLOYDS engaged in a systematic practice of ‘stripping’ wire transfer information. Stripping is the practice of removing wire transfer information that would identify that the transfers originated from a prohibited source. By stripping out the originator information, the wire transfers could pass through the screening software used by New York banks that would otherwise have rejected or frozen them for further inquiry. The stripping of wire transfer information in this manner made it appear that the transactions originated at LLOYDS in the United Kingdom rather than the sanctioned banks. … Beginning in the mid-1990s, LLOYDS began removing any information from Iranian and Sudanese wire transfers that would trigger the detection systems at New York correspondent banks. To execute this policy, LLOYDS personnel removed any information that identified the payment messages as originating from Iranian, Sudanese or other sanctioned countries. The falsified wire transfers would then be processed undetected by the OFAC filters in place at the U.S. banks.

According to the Factual Statement appended to the DPA, Lloyds maintained correspondent accounts in London for Iranian banks and had a formal process for pulling Iranian SWIFT messages destined for U.S. banks out of its outbound message queue, marking them up by hand in hard copy to eliminate references to Iran, and then re-keying the messages into its own system, making the messages appear to originate from Lloyds. The Factual Statement also indicates that Lloyds engaged in similar conduct in its branches in several other countries, and on behalf of other sanctioned entities, but on a more ad hoc basis.

The Factual Statement further states that «Lloyds’s actions caused U.S. banks to provide services to . . . sanctioned countries, and falsified business records of banks primarily located in New York, New York.»39 Accordingly, Lloyds accepted responsibility for violating both IEEPA and NY Penal Law §§ 175.05 and 175.10 that, «with the intent to defraud,» make it a crime to «(i) make or cause a false entry in the business records of an enterprise . . . or (iv) prevent the making of a true entry or cause the omission thereof in the business records of an enterprise.»40 According to the Factual Statement, none of the transactions were processed through Lloyds’s own U.S. offices.

Pursuant to the DPA, Lloyds agreed, among other things, to (i) adopt best practices for anti-money laundering and combating terrorist financing as well as the Wolfsberg Anti-Money Laundering («AML») Principles for Corresponding Banking,41 (ii) cooperate with ongoing investigations, and (iii) pay the sum set forth above. If Lloyds abides by the terms of the DPA and cooperates fully with the ongoing investigations, the DOJ will dismiss the information in 2 years.

1.3 Questions to Help Identify Potential OFAC Exposure to Non-U.S. Financial Institutions

Based on the foregoing discussion, non-U.S. financial institutions may wish to consider the following questions to help evaluate whether they are involved in activities that may give rise to risk of OFAC-related exposure:

- Does the institution engage in dollar clearing transactions through U.S. correspondent banks that may involve OFAC sanctioned parties or OFAC prohibited activities?

2. The Anti-Terrorism Act

The ATA makes it a crime deliberately to provide certain support for terrorist activities or to terrorist organizations, and creates a civil action and federal jurisdiction for recovery of treble damages and attorneys’ fees for any U.S. national injured in his or her person, business or property by an act of international terrorism. It also makes it a crime to deliberately provide material support or resources to designated terrorist organizations or terrorist activities. In institutions that answer any of the foregoing questions in the affirmative should ensure, with the assistance of outside counsel familiar with OFAC issues, that they have in place adequate policies and procedures to address and mitigate any potential OFAC-related exposure.

Institutions that answer any of the foregoing questions in the affirmative should ensure, with the assistance of outside counsel familiar with OFAC issues, that they have in place adequate policies and procedures to address and mitigate any potential OFAC-related exposure.

Does the institution ever use cover payments to allow its U.S. correspondent banks to process payments through the United States that otherwise would be flagged by its U.S. correspondent’s OFAC filters?

Does the institution engage in transactions regardless of currency with countries, entities, or individuals subject to U.S. sanctions on behalf of U.S. persons, or in transactions that have any other nexus to the United States?

Are any U.S. citizens or residents employed by the institution outside the United States, particularly in positions in which they are responsible for financial transactions?

Private civil plaintiffs injured by acts of international terrorism (e.g., attacks perpetrated by Hamas, Hezbollah, and the PLO) have brought suit against numerous banks under the ATA, alleging expansive (and dubious) theories of liability under the ATA, e.g.: (1) the defendant banks violated the ATA’s criminal provisions either by maintaining accounts for, or clearing wire transfers to or from, organizations that certain countries (e.g., the United States, Israel) or other sources (e.g., news accounts, internet sites) supposedly identified as terrorists or “fronts” for terrorists; (2) thereafter, the plaintiffs were injured by an attack perpetrated by a terrorist organization; and (3) therefore, the banks are liable under the ATA for plaintiffs’ injuries.

The following are the underlying criminal violations of the ATA on which plaintiffs have sought to premise civil liability:

1. 18 U.S.C. § 2339A (Providing Material Support to Terrorists) makes it a crime to “knowingly provide[] material support or resources” to any organization designated as a terrorist organization by the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General.

2. 18 U.S.C. § 2339B (Providing Material Support or Resources to Designated Foreign Terrorist Organizations) makes it a crime to “knowingly provide[] material support or resources” to an entity that the U.S. Government has designated as a FTO.

3. 18 U.S.C. § 2339C (Prohibition Against the Financing of Terrorism) makes it a crime to “directly or indirectly, unlawfully and willfully provide[] funds with the intention that such funds be used, or with the knowledge that such funds are to be used, in full or in part, to cause death or serious bodily injury to a civilian or in furtherance of certain other enumerated crimes.”

2.1 Potential Extraterritorial Effects for Non-U.S. Financial Institutions

The criminal provisions found in 18 U.S.C. § 2339B and § 2339C contain rules providing for these sections to apply to offenses having occurred outside of the United States if, among other things, the offense was directed at a U.S. person, or the defendant can be “found” in the United States. Under a more favorable reading of the statute, a non-U.S. bank should not be deemed to be “found” in the United States for these purposes merely...

42 The term “cover payment” refers to a method of processing international funds transfers in which the originating bank in a funds transfer sends two payment messages to affectuate the funds transfer requested by its customer. One message (MT-103) is sent to the beneficiary customer’s bank (the beneficiary bank) containing the full details of the payment routing, i.e., information on the originating customer and beneficiary customer, their banks, and intermediate clearing banks; the other message (MT-202) is sent by the originating bank to its correspondent bank and only includes the names of the originating bank, the beneficiary bank and, if necessary, the name of the correspondent bank of the beneficiary bank. The second message allows the originating bank’s correspondent bank to make a payment to the beneficiary bank’s correspondent bank which in effect “covers” the payment and allows the beneficiary bank to credit its customer (i.e., the beneficiary of the funds transfer).


44 18 U.S.C. § 2333(a) Civil Remedies Action and Jurisdiction. – “Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefore in any appropriate district court of the United States and shall recover therefor the damages he or she sustains and the cost of the suit, including attorney’s fees.”

because it has a U.S. branch, however, U.S. courts have yet to definitively resolve this issue.

As for the ATA’s civil provisions, and the litigation costs and potential exposure that treble damages pose, plaintiffs have brought suit against non-U.S. banks based on allegations that the banks provided only routine banking services, entirely outside of the United States, to entities that have been designated as or accused of being terrorist fronts only by non-U.S. governments or news sources. Thus far, such plaintiffs have yet to win a judgment against banks sued under these expansive—and in many respects, legally incorrect—readings of the ATA. However, some civil complaints based on such broad reading of the ATA have survived initial challenges at the motion to dismiss stage of U.S. litigation, and have progressed to pretrial discovery.

2.2 Case Study: NatWest

On September 29, 2005, a group of 83 plaintiffs, primarily U.S. citizens resident in Israel who were victims of HAMAS terrorist attacks in Israel, or relatives of such victims, brought suit against National Westminster Bank, London (“NatWest”) in the United States District Court for the Eastern District of New York (i.e., in federal court in Brooklyn, New York), asserting claims under Section 2333 (civil remedies) of the ATA based on allegations that NatWest had provided material support for acts of terrorism in violation of Section 2339B and financed terrorism in violation of Section 2339C.

The complaint alleged that NatWest committed those acts, first and foremost, by knowingly maintaining, for a period of nine years, an account relationship with an entity known as Interpal. Interpal holds itself out as a charity, but was first suspected of funneling funds to Hamas in 1996. In 1998, Israel designated Interpal as a terrorist organization, and in 2003, the United States designated Interpal as a SDGT. The attacks that the NatWest plaintiffs alleged mostly occurred after the Israeli designation, but before the United States had listed Interpal as an SDGT. The plaintiffs also alleged that NatWest processed funds transfers between Interpal and other organizations allegedly linked to HAMAS (e.g., the Jenin Committee, the Tulkarem Committee and the Holy Land Foundation), none of which were alleged to be direct customers of NatWest.

On January 26, 2006, NatWest moved to dismiss the complaint for failure to state a claim and on September 29, 2006, the court denied the motion as to NatWest’s claims for violation of the ATA based on allegations that NatWest committed underlying violations of 18 U.S.C. §§ 2339B and 2339C.46

The court held that to allege a violation of Section 2339B, plaintiffs had to allege three elements, i.e., that NatWest provided (1) material support; (2) to a U.S. designated FTO; and (3) knowingly.

First, the court held that providing financial services, even if only routine services such as processing funds transfers for an entity that is not a bank customer, could constitute the provision of «material support» as that term is used in the ATA.

Second, the court held that three of the entities named in the complaint (the Jenin Committee, the Tulkarem Committee and the Holy Land Foundation), although not designated by the United States as FTOs, were the equivalent of FTOs for purposes of a violation of Section 2339B, because they were allegedly controlled and dominated by Hamas, which was an FTO. The court concluded that based on the allegations in the complaint, two organizations, including Interpal (the only one of these entities for which NatWest was alleged to have maintained an account) were not FTOs.

Third, the court held that plaintiffs’ allegations were sufficient to establish that NatWest had knowingly supplied material support to the foregoing FTOs. Notably, the plaintiffs did not directly allege facts showing that NatWest did, in fact, have actual knowledge that the Jenin Committee, the Tulkarem Committee and the Holy Land Foundation were linked to Hamas. Instead, the complaint alleged that the Israeli government had labeled the Jenin Committee and the Tulkarem Committee as «unlawful organizations,» and identified the Holy Land Foundation as a Hamas front group. The complaint also alleged that NatWest’s own bank policy required the bank to «monitor publicly available information and allegations about the organizations from which its customers receive funds, and to which its customers transfer funds.» The court held that NatWest could be deemed to have knowledge that the Jenin Committee, the Tulkarem Committee and Holy Land Foundation were fronts for Hamas based on the Israeli designations, which, according to the court, NatWest could be presumed to know—at least at the initial stages of the case—based on its policy to monitor «publicly available» information. Furthermore, the court suggested (but did not clearly decide) that even if NatWest’s own policies did not impose a burden of knowledge upon it, the same result could be supported based on the argument that the Wolfsberg Principles and/or the FATF guidelines required it to review the relevant Israeli lists.

To allege a violation of Section 2339C, the court held that the plaintiffs had to allege that NatWest: (1) provided or collected funds; (2) with the knowledge that the funds would be used to promote a terrorist act. The court took a broad view of what it means to provide or collect funds, under which not just donating funds to

---

terrorists, or fund raising for terrorists, is covered, but moreover opening an account or processing funds transfers, fall within the scope of the prohibition. As for the knowledge that the funds would be used for a terrorist act, the court took the same view as described above – if there was publicly available information suggesting a group’s terrorist purpose, NatWest could be deemed familiar with such information by virtue of its policies. According to the court, publicly available knowledge might include not just government designations, but also information on the website of an allegedly terrorist organization, or even news articles. The court held that NatWest would be deemed to have knowledge of Interpal’s terrorist purposes based on such factors, as well as the fact that U.K.’s Charity Commission had frozen Interpal’s assets in 1996 based on suspicions of ties to terrorism, notwithstanding the fact that the Charity Commission had ultimately unfrozen the funds.

Following the court’s ruling, the case has now progressed to the discovery stage, after which NatWest will have an opportunity to contest on the merits the facts alleged in the complaint (which were presumed to be true for the purposes of the motion to dismiss at the outset of the case). At the conclusion of the case, if NatWest does not prevail, it also will have an opportunity to appeal the trial court’s legal rulings, many of which NatWest will have strong arguments against. At best, however, it will be time consuming and expensive for NatWest to vindicate its position.

2.3 Questions to Help Identify Potential ATA Exposure to Non-U.S. Financial Institutions

Based on the foregoing discussion, a non-U.S. financial institution may wish to consider the following questions to help evaluate whether it is adequately protected with regard to the risk of ATA-related exposure:

- Does the institution have in place procedures (including computer screening based on names supplied by a reliable vendor) to ensure that it does not wire funds to or from, or maintain accounts for, persons or entities identified by the United States, Israel, other countries, the U.N., or international organizations as being a terrorist, or terrorist-affiliated person or entity?

- Does the institution have in place policies and procedures designed to mitigate the risk that it will be deemed, based on publicly available information such as websites and news articles, to have knowledge of whether its customer’s customers (e.g., wire transfer recipients with no customer relationship with the bank) may be terrorist fronts?

Institutions that answer either of the foregoing questions in the negative may wish, with the assistance of outside counsel familiar with ATA issues, to update their policies and procedures better to address potential ATA risk.

3. The Alien Tort Statute

The ATS provides that “[t]he district courts shall have original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States.” Under the ATS, non-U.S. persons – and only non-U.S. persons – may bring civil suits in U.S. courts for injuries they suffered due to alleged violations of international law that occurred entirely outside of the United States.

In 2004, the Supreme Court addressed the ATS for the first time since its enactment in 1789 as part of the Judiciary Act. The Court held that the ATS is a jurisdictional statute that “enabled federal courts to hear claims in a very limited category defined by the law of nations and recognized at common law.” The Supreme Court further instructed that, before recognizing any new category of ATS claim, a court must determine whether the alleged violation has “definite content and acceptance among civilized nations” equivalent to those of the limited number of 18th-century violations (such as piracy) that the statute was enacted to address. Despite these limitations on recognizing new ATS claims, a number of lower U.S. courts have recognized a civil claim for aiding and abetting liability under the ATS. The recognition of aiding and abetting liability represents a significant expansion of the potential reach of the ATS. Most international law prohibitions can be violated only by governmental action, and not by private parties. However, if plaintiffs are permitted to pursue claims based on the theory that private actors aided and abetted governmental conduct that violates international law, only when committed by a government (e.g., apartheid, extrajudicial killing), plaintiffs have a potential means to impose liability against private defendants for conduct that, if committed by private actors themselves, would not be actionable.

49 Id. at 712.
50 Id. at 732.
51 See, e.g., Khulumani v. Barclays Nat’l Bank, 504 F.3d 254 (2d Cir. 2007). In Khulumani, putative classes effectively representing all victims of South African apartheid sued over 50 corporate defendants, alleging that by doing business in apartheid-era South Africa, the defendants aided and abetted apartheid in violation of international law, giving rise to a cause of action under the ATS. The trial court dismissed, holding that aiding and abetting claims are not cognizable under the ATS. In re South African Apartheid Litig., 346 F. Supp. 2d 538, 549 (S.D.N.Y. 2004). On appeal, two judges on the three judge panel voted to reverse, but disagreed as to the proper standard for aiding and abetting liability. A third judge dissented, taking the view that the ATS does not recognize a claim for aiding and abetting apartheid.
In recent years, ATS litigation has blossomed, particularly against global corporations that allegedly aided and abetted violations of international law by governments other than the U.S. government. To provide just a few examples, plaintiffs have sued: (i) the Vatican Bank, based on allegations that it aided and abetted war criminals at the end of World War II by helping them evade prosecution and preserve looted assets; (ii) DaimlerChrysler AG, based on allegations that it aided and abetted the Argentinean police and military in murdering labor protesters and union officials and/or causing their disappearance; (iii) Caterpillar, based on allegations that it sold bulldozers to the Israeli military that were used to demolish Palestinian homes; (iv) Exxon Mobile Corp., based on allegations that it had been complicit in human rights abuses committed by Indonesian security forces protecting a natural gas extraction facility and pipeline that Exxon was operating; and (v) Coca-Cola, based on allegations that its Colombian bottler aided and abetted paramilitary actions taken in Colombia against labor union members.

Plaintiffs have obtained some high dollar settlements on ATS claims and have imposed significant litigation costs on defendants who have litigated (or are still engaged in litigation), but generally plaintiffs have not, or at least not yet, prevailed in reaching final, favorable judgments on an aiding and abetting theory under the ATS.

### 3.1 Potential Extraterritorial Effects for Non-U.S. Financial Institutions

In the narrower context of anti-terrorism finance, plaintiffs have sued financial services firms based on allegations that the banks aided and abetted violations of international law perpetrated by others.

A non-U.S. bank that is amenable to U.S. jurisdiction (e.g., that has a U.S. branch or that routinely conducts substantial, ongoing business in a U.S. forum) therefore may be subject to civil suits in U.S. courts, brought by non-U.S. persons based on the bank’s actions entirely outside of the United States, and premised on the theory that the bank’s routine banking activity aided and abetted terrorism or human rights violations committed by governments or others.

#### 3.2 Case Study: Arab Bank PLC

In Almog v. Arab Bank PLC, certain non-U.S. plaintiffs who were victims of terrorist acts in Israel during the second Intifada in late 2000, filed ATS claims against Arab Bank, a Jordanian bank, alleging that the bank aided and abetted the terrorist attacks against them by, among other things, maintaining accounts for Hamas, other terrorist organizations, and individual supporters of terrorist organizations.

On January 29, 2007, the court denied Arab Bank’s motion to dismiss the complaint against it, holding that plaintiffs’ allegations were sufficient to state a claim under the ATS and paving the way for the case to proceed to the discovery stage. In denying Arab Bank’s motion to dismiss, the court first held that the Hamas attacks on the plaintiffs were violations of international law prohibitions against genocide and crimes against humanity. In holding that terrorist attacks were tantamount to genocide and crimes against humanity, the court relied heavily on the fact that Hamas and other terrorist organizations acted with the “shared mission to eradicate the State of Israel” and “murder or throw out the Jews.” The court also held that Hamas’s conduct violated an international law prohibition against “suicide bombings” and “other murderous attacks on innocent civilians” that are “intended to intimidate or coerce a civilian population.” In so holding, the court relied on, among other things, the International Convention for the Suppression of Terrorist Bombings and the provisions of the Financing Convention that make it an offense to finance, among other things, acts covered by the Bombing Convention.

The court next turned to the question of whether Arab Bank could be held secondarily liable based on allegations that Arab Bank aided and abetted the terrorist attacks by Hamas and others. The court held that a claim for aiding and abetting genocide, crimes against humanity, and suicide bombings would be cognizable under the ATS, relying in large part on the conclusion...
that «the Genocide, Bombing, and Financing Conventions explicitly condemn acts of complicity or aiding and abetting by non-primary actors.»

As to the elements of the aiding and abetting claim, the court held that «the actus reus of aiding and abetting in international criminal law requires practical assistance, encouragement, or moral support which has a substantial effect on the perpetration of the crime,» and that as to requisite mental state, «knowledge that [the bank’s services] are supporting unlawful acts» would suffice. Plaintiffs’ allegations that Arab Bank had maintained accounts for Hamas, and for terrorist front organizations, with knowledge of their terrorist purposes, therefore were sufficient, in the court’s view, to survive a motion to dismiss at the outset of the case. The court rejected Arab Bank’s argument that its provision of routine banking services should not be actionable, holding that even activities that may themselves be benign may be actionable if done with knowledge that they are supporting unlawful acts.

3.3 Questions to Help Identify Potential ATS Exposure to Non-U.S. Financial Institutions

Based on the foregoing discussion, a non-U.S. financial institution may wish to consider the following questions to help evaluate whether it is adequately protected with regard to the risk of ATS-related exposure:

• Does the institution have policies and procedures governing when and how it may do business in or with countries that may be perceived as state sponsors of terrorism? Does the institution have a system for monitoring activity in such accounts once opened to provide it with a reasonable comfort level that such accounts are not being used for terrorist activity?

• Does the institution have policies and procedures to help ensure that it is not doing business with individuals and entities that may be alleged to have committed acts of terrorism, acted as fronts for terrorist organizations, or otherwise provided support to terrorists?

Institutions that answer either of the foregoing questions in the negative may wish, with the assistance of outside counsel familiar with ATS issues, to update their policies and procedures better to address potential ATS risk.

III. Conclusion

As described above, in the wake of 9/11, U.S. prosecutors and civil plaintiffs have used a wide range of both new and existing tools in an effort to impose liability, not just against those that directly raise funds for, and donate their own funds to, terrorists, but also against certain financial institutions based on their routine provision of banking services. Often such cases are premised on flimsy, and likely unsupportable, allegations of knowledge that such banking services in fact were supporting terrorists or their front companies. Indeed, in some cases, the banks’ customers were not blacklisted in the bank’s home jurisdiction nor the customers’ home jurisdictions (only in the United States, if anywhere). And, as noted, in many cases, the services the banks were alleged to have provided occurred only outside the United States. But none of those facts is a guaranteed defense; indeed, as some courts have interpreted the law, those facts may not be a defense at all.

Accordingly, compliance policies and procedures designed to mitigate risks with respect to a financial institution’s activities – even if conducted by its non-U.S. employees or by its non U.S. operations – should address extraterritorial effects of U.S. anti-terrorism finance laws. Financial institutions should consider carefully the questions set forth above – that are designed to help them identify their potential exposure to U.S. anti-terrorism laws – and take steps to address through their policies and procedures any risks identified.