New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
DECEMBER 3, 2014

Combating Terrorist Financing

By **David I. Miller and Brianna Abrams**

The 24-hour news cycle provides a constant reminder of the threats posed by the Islamic State in Iraq and Syria (ISIS) and Al-Qaeda affiliated groups. Unlike many other terrorist groups, however, ISIS has considerable financial resources at its disposal. On Oct. 23, 2014, the Under Secretary of Treasury for Terrorism and Financial Intelligence, David Cohen, noted that ISIS raises tens of millions of dollars a month.[1] As Cohen emphasized, "[W]e at the Treasury Department are intensifying our focus on undermining [ISIS's] finances."

The U.S. government has indicated that it will use all tools at its disposal to cut off ISIS's financial network and act against entities, including financial institutions, that are conduits to fund terrorist activities. Indeed, since Sept. 11, 2001, financial institutions have faced increased scrutiny for their often-unwitting role in terrorist financing. The myriad of laws and regulations that govern this area require diligence to avoid potential criminal and civil liability. This article outlines the applicable laws and regulations, discusses recent civil and criminal action in this area, and offers suggestions to try and avoid the crosshairs of government authorities and private litigants.

Applicable Laws

Over the last four decades, Congress and the president have devised several mechanisms to choke the lifeblood of criminal enterprises: money. These laws include the Bank Secrecy Act (BSA), Anti-Money Laundering laws (AML), the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), the International Emergency Economic Powers Act (IEEPA), and criminal statutes proscribing money laundering and terrorism-related activities.

The cornerstone of the government's effort to combat the financing of criminal activity is the BSA, which imposes stringent requirements on financial institutions to monitor and report potentially suspicious customer activity.[2] The BSA was designed to help identify, inter alia, the laundering of money deposited into U.S. financial institutions. Traditionally, money laundering involved making illegal proceeds ("dirty money") appear legal ("clean money") by introducing dirty money into the legitimate financial system, often through the use of foreign bank accounts.[3]

The BSA assists authorities in tracking illicit funds through the use of reporting forms such as Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). CTRs must be filed for all transactions

David I. Miller and Brianna Abrams

greater than $10,000.[4] Generally, a financial institution must file a SAR for bank transactions involving $5,000 or more if the bank knows or suspects that the transaction: (1) involves, or is intended to hide, funds derived from illegal activities; (2) is designed to evade BSA regulations; (3) has no apparent lawful purpose; or (4) is an abnormal transaction for a particular customer with no reasonable explanation.[5]

Information from CTRs and SARs is maintained in a database administered by the Financial Crimes Enforcement Network (FinCEN), a bureau within the U.S. Treasury Department. Law enforcement, financial regulators, and the intelligence community can access the database to identify possible terrorist financing and money laundering. Because of the importance of CTRs and SARs, the government has stressed the need for filing compliance.[6] Furthermore, the above BSA provisions work in connection with AML laws criminalizing money laundering activity,[7] strengthening penalties for money laundering,[8] and

enhancing the reporting and compliance requirements for financial institutions.[9]

Since the 1990s, Congress has enacted a number of statutes criminalizing terrorist financing. Two of the key enforcement tools were added in 1994 and 1996, when Congress criminalized the provision of "material support" to enumerated terrorist-related activities or to a designated foreign terrorist organization (FTO).[10] Currently, there are 59 groups designated as FTOs by the State Department.[11] For financial institutions, providing "material support or resources" can mean providing banking and/or wire services to an FTO.[12] Indeed, banks are required to seize any funds in their possession in which a terrorist organization has an interest.[13] Further, Congress has criminalized the provision of funds to terrorists with knowledge that such funds will be used to carry out certain violent acts.[14] Congress has also provided a private civil remedy to any U.S. national "injured…by reason of an act of international terrorism."[15]

Following 9/11, the USA PATRIOT Act bolstered BSA and AML enforcement. The act imposed more stringent procedures and requirements on financial institutions, including tougher prohibitions against business activities with foreign shell banks and enhanced due diligence procedures for private banking accounts.[16] Additionally, other enforcement tools, including IEEPA, have enabled the president to block or restrict transactions with targeted countries, organizations, and individuals.[17] Several presidential executive orders, including Executive Orders 13224, 13099, and 12947, prohibit financial transactions with designated individuals and groups known as Specially Designated Global Terrorists (SDGTs) and organizations designated as Specially Designated Terrorists (SDTs).[18]

The Office of Foreign Asset Control (OFAC) of the Department of Treasury maintains a list of FTOs, SDGTs, SDTs, and other individuals and entities that are targets of U.S. economic sanctions—collectively, these targets are known as Specially Designated Nationals (SDNs).[19] The Department of Justice has pursued sanctions and criminal charges against banks that transact business with SDNs. Notably, the government has also prohibited, and aggressively prosecuted, financial transactions with four countries that have been designated as state supporters of international terrorism: Cuba, Iran, Sudan, and Syria.[20]

Recent Litigation

Over the last decade, government authorities and civil litigants have used the aforementioned laws to combat terrorist financing more forcefully. While there are several notable examples, we identify three cases that illustrate the efforts financial institutions should take to avoid being used as an instrument of terror.

Using the private right of action created under the Antiterrorism Act, civil litigants in *Linde v. Arab Bank*, CV-04-2799 (NG)(VVP) (E.D.N.Y.), sought redress against a Jordanian bank claiming it had actual knowledge that customers' funds were used to facilitate terrorist attacks. *Linde* represents the first lawsuit brought under the Antiterrorism Act to reach a trial verdict against a financial institution, and the verdict was unfavorable for the bank.

The plaintiffs were hundreds of U.S. nationals and family members who were victims of international terrorist attacks. They claimed that Arab Bank materially supported the efforts and goals of terrorist organizations, including Hamas, by providing banking services for those organizations—knowing that the accounts were being used to facilitate terrorist attacks—and for charities that Arab Bank knew were affiliated with those organizations or were fronts for them. The plaintiffs also alleged that Arab Bank administered the financial infrastructure by which the Saudi Committee for the Support of the Intifada Al Quds (the Saudi Committee) distributed benefits to the families of "martyrs."[21]

At trial, the bank argued it provided routine financial services and in no way "knowingly" supported a terrorist organization. It presented evidence of its AML compliance program, including the use of automated screening systems that incorporate OFAC sanction lists. The plaintiffs' case was built on the theory that "when a bank opens its doors to terrorists, they're going to be held accountable."[22] The plaintiffs highlighted the inadequacy of the bank's compliance program with testimony that bank representatives had seen documentation specifically referencing "martyr" payments. A critical issue arose during discovery when the bank argued that foreign bank secrecy laws prevented the production of certain customer account records. After years of refusing to produce the records, the court imposed adverse inference sanctions.[23]

At trial, the court instructed the jury that because of the bank's nonproduction of customer records, the jury could infer that the bank knowingly provided financial services to

Hamas and it processed payments on behalf of the Saudi Committee to terrorists, including those affiliated with Hamas.[24] The court also gave an instruction that the jury could find that Arab Bank acted "knowingly" if the bank was willfully blind to a fact. On Sept. 22, 2014, after only two days of deliberations, the jury returned a verdict in favor of the plaintiffs, finding Arab Bank liable for knowingly supporting terrorism.

The same day as the Linde verdict, the U.S. Court of Appeals for the Second Circuit held in *Weiss v. National Westminster Bank*[25] that there is no requirement that a bank knowingly aid terrorist activities to be liable under the Antiterrorism Act. The plaintiffs in *Weiss* were 200 U.S. nationals, estates or heirs who were victims of Hamas terrorist attacks. They claimed that the defendant bank provided material support and resources to Hamas by maintaining bank accounts and transferring funds for a non-profit organization, Palestine Relief & Development Fund, a/k/a Interpal (Interpal), which allegedly solicited funds and otherwise provided support for Hamas.

Before the district court, the bank won summary judgment by arguing that the plaintiffs had not shown that the bank had knowledge of, or exhibited deliberate indifference to, whether Interpal funded terrorist activities.[26] In reversing the district court's decision, the Second Circuit relied on the Supreme Court's decision in *Holder v. Humanitarian Law Project*,[27] which held that under 18 U.S.C. §2339B, the requisite mental state is "knowledge about the organization's connection to terrorism, not specific intent to further the organization's terrorist activities."

The Second Circuit concluded that the plaintiffs were only obliged to show that the bank knew (or exhibited indifference) that Interpal provided material support to a FTO, i.e. Hamas, not that the bank knew (or exhibited indifference) that Interpal's support aided Hamas's terrorist activities, and found that the plaintiffs had presented genuine issues of fact on this issue.[28]

An example of criminal enforcement is the Justice Department's prosecution of the largest Muslim charity in the United States: *United States v. Holy Land Foundation for Relief & Dev.*, No. 3:04–CR–0240–P (N.D. Tex.). Holy Land Foundation for Relief & Development (HLF) was declared a Specially Designated Terrorist in 2001. In 2004, a grand jury indicted HLF for providing funding to Hamas's Social Wing and using HLF funds to support the families of suicide bombers. Several banks that HLF used were subpoenaed during the Justice Department's investigation. In November 2008, after a mistrial and lengthy retrial, HLF and individual defendants were found guilty of multiple terrorism-related charges.[29]

Recommendations

The above discussion demonstrates that robust BSA/AML compliance programs may be critical defense tools in avoiding enforcement actions and civil lawsuits alleging support for terrorist financing. The following are ways in which financial institutions may consider bolstering their compliance programs to defend against claims of "knowingly" providing material support to a terrorist organization.

First, a financial institution may consider utilizing automated monitoring technology that searches whether customers are on governmental lists of FTOs, SDGTs and SDNs, or are transacting with entities or individuals on the lists. As the Linde trial showed, however, an automated compliance program may be insufficient.

Second, a robust Know-Your-Customer program is recommended. In order to comply with the terrorist financing laws, financial institutions should consider creating comprehensive Customer Identification Programs (CIP) and perform requisite customer due diligence (CDD). CIP compliance involves collecting and verifying customer information and thorough record-keeping. Institutions may also consider performing CDD by identifying beneficial owners; understanding customer relationships; and monitoring and updating customer information.

Factors to consider when evaluating a customer's risk level include the nature of the customer's business, the geography of the business, and the banking products used. High-risk factors may include: cash-intensive account activity; entities controlled by offshore, private entities; private trust accounts; and fund transfers to or from high-risk countries, including countries embroiled in armed conflict. Striking a balance between due diligence and jeopardizing client relations may be a delicate task, but due diligence should be commensurate with the perceived level of risk.

Third, a financial institution should monitor and report suspicious activity and file SARs in a timely, comprehensive fashion. Financial institutions should pay close attention to the source of funds and to suspicious money transfers.

Finally, bank representatives should be willing to perform enhanced due diligence and question potential connections to terrorist organizations even where it could jeopardize client relationships.

Conclusion

The landscape of terrorist financing laws and regulations can be a veritable minefield for financial institutions to navigate. In implementing strong compliance steps, however, banks and other institutions can better safeguard against government enforcement actions and potential private party lawsuits. Given large-scale terrorist financing activity for the foreseeable future — including for groups like ISIS — diligent monitoring and preventive measures are necessary to avoid damaging enforcement actions and private litigation.

1. See Remarks of Under Secretary for Terrorism and Financial Intelligence David S. Cohen at The Carnegie Endowment for International Peace, "Attacking ISIL's Financial Foundation," Oct. 23, 2014, available at http://www.treasury.gov/press-center/press-releases/Pages/jl2672.aspx.
2. See 31 U.S.C. §5311 et seq.
3. Legal and Economic Impact of Foreign Banking Procedures on the United States: Hearing before the House of Representatives Comm. on Banking and Currency (Dec. 9, 1968) (statement by Rep. Patman, Chairman, House Comm. on Banking and Currency).
4. 31 C.F.R. §1010.311.
5. 12 C.F.R. §353.3.
6. See, e.g., Remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, on Aug. 12, 2014 (noting that BSA-required information reported in preceding month is directly relevant to 1,100 ongoing FBI investigations) available at http://www.fincen.gov/news_room/speech/html/20140812.html.
7. Money Laundering Control Act of 1986, P.L. 99-570.
8. Annunzio-Wylie Anti-Money Laundering Act of 1992, P.L. 102-550.
9. See e.g., Money Laundering Suppression Act of 1994, P.L. 103-3235 and Money Laundering and Financial Crimes Strategy Act of 1998, P.L. 105-310.
10. See 18 U.S.C. §§2339A and 2339B.
11. See "Foreign Terrorist Organizations" available at http://www.state.gov/j/ct/rls/other/des/123085.htm.
12. Notably, in investigating terrorist financing, the enforcement discussion has shifted from a dirty-money-versus-clean-money analysis to a focus on the application of funds, regardless of the source.
13. 18 U.S.C. §2339B(a)(2). Failing to comply with the seizure requirement can result in civil penalties. 18 U.S.C. §2339B(b).
14. 18 U.S.C. §2339C.
15. 18 U.S.C. §2333(a).
16. See e.g., USA PATRIOT Act, Title III, Section 311 et seq. (referred to as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001).
17. See 50 U.S.C. §§1701-1707; 31 C.F.R. §596.201.
18. The Department of Treasury has promulgated regulations detailing which individuals, groups, and entities may be designated SDGTs—they are those listed in the referenced executive orders and designated by the Secretary of State, in consultation with the Secretary of Homeland Security, the Attorney General, and the Secretary of the Treasury. See 31 C.F.R. §§594.201 and 594.310.
19. See "Specially Designated Nationals & Blocked Persons" at http://www.treasury.gov/ofac/downloads/t11sdn.pdf.
20. See, e.g., 31 C.F.R. §596.201.
21. *Linde v. Arab Bank*, 269 F.R.D. 186, 191-92 (E.D.N.Y. 2010).
22. Bernard Vaughan, "Arab Bank liable over Hamas attacks: U.S. jury" Reuters, Sept. 22, 2014, quoting Mark Werbner, a lawyer for some of the plaintiffs.
23. *Linde*, 269 F.R.D. at 202, 205.
24. Id.; Final Jury Charge at 14, *Linde*, 04 Civ. 2799 (E.D.N.Y. Sept. 17, 2014) (Dkt. No. 1162).
25. 768 F.3d 202 (2d Cir. 2014).
26. Id. at 205.
27. 561 U.S. 1 (2010).
28. *Weiss*, 768 F.3d at 205-06, 211-12.
29. In a related civil case against HLF, the family of a teenager killed by Hamas sued HLF and was awarded $52 million, which was trebled to $156 million. Final Judgment Order, *Boim v. Holy Land Found. for Relief & Dev.*, Case: 1:00-cv-02905 (N.D. Ill. Oct. 12, 2012) (Dkt. No. 889).

David I. Miller *and* ***Brianna Abrams*** *outline the laws and regulations that govern financial institutions often-unwitting role in terrorist financing, discusses recent civil and criminal action in this area, and offers suggestions to try and avoid the crosshairs of government authorities and private litigants.*