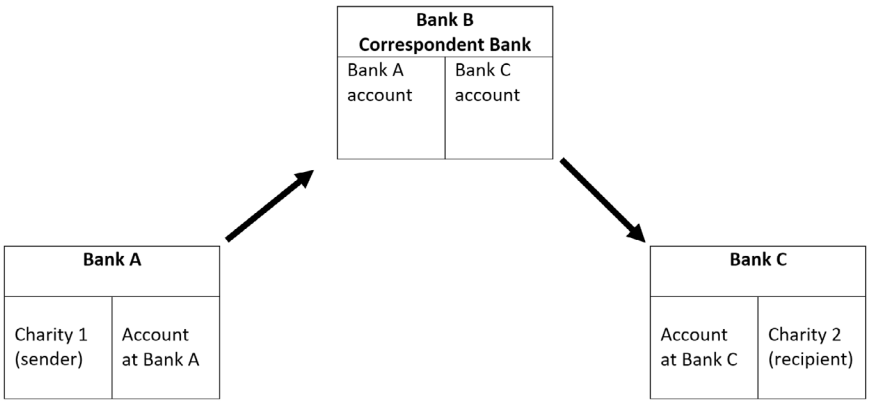
Chapter 2
THE CONTEXT FOR NPO FINANCIAL ACCESS PROBLEMS

A variety of forces shape the complex environment in which financial institutions operate, affecting how they deal with the needs of their NPO customers whose work requires transferring funds to staff, partner NPOs and vendors in other countries. These forces include the regulatory structure for both FIs and NPOs, U.S. AML/CFT policies, and enforcement actions. The way FIs respond to these forces has contributed to narrowing access to financial services for NPOs.

Overview of International Financial Transactions: Correspondent Banking and SWIFT[23]

To comprehend the reasons NPOs are having difficulties with financial services, a basic understanding of how the international financial system works is necessary. International financial transactions rely on a system of "correspondent" banking relationships. A correspondent bank serves as the intermediary between the bank sending a transfer on behalf of a client (retail bank) and the bank issuing payment to the recipient (respondent bank). Both the retail and correspondent bank hold an account at the correspondent bank, which is used for fund transfers, cash management and other purposes. It is the bedrock of international finance and trade.

Figure 1: Basic Process for Cross-Border Financial Transfers



Written agreements between the retail bank and correspondent bank establish the process for payments among the retail bank and its customers. During an international transfer, retail FIs forward payment instructions to the correspondent bank to sort and process. To provide for secure and consistent communication among banks, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network enables financial institutions to send and receive information and instructions through a standardized system of codes.

23 Based on Bank for International Settlements, Committee on Payments and Market Infrastructures, "Correspondent Banking," July 2016, http://www.bis.org/cpmi/publ/d147.pdf.

SWIFT is the largest messaging network, used by more than 11,000 financial institutions in more than 200 countries and territories.[24] SWIFT does not hold funds or manage accounts on behalf of customers, but rather enables users to communicate securely, exchanging standardized financial messages in a reliable way, thereby facilitating global financial flows. SWIFT sends payment orders that are settled through correspondent accounts that institutions maintain with each other.

In the past several years, the number of correspondent banking relationships has declined, especially for respondent banks that are located in higher-risk jurisdictions (those subject to sanctions), for customers perceived as higher risk (such as NPOs), or for customers who generate revenues insufficient to recover compliance costs. Increased regulatory compliance costs and penalties, especially concerning AML/CFT requirements, and reduced risk appetite by FIs have been attributed as the drivers for the reduction in correspondent banking.[25]

The ability to make and receive international payments via correspondent banking is vital for businesses, NPOs and individuals, as well as global economic growth. A decline in the number of correspondent banking relationships affects the ability to send and receive international payments and could drive some payment flows underground, with potential consequences on growth, financial inclusion, and the stability and integrity of the financial system.[26] In recognition of these concerns, analytical work has been undertaken by several intergovernmental agencies, including the FSB and International Monetary Fund (IMF), and some governments, notably the UK,[27] to understand the withdrawal of correspondent banking and remittances.

Legal Authorities

The U.S. maintains an extensive system of sanctions on various countries and non-state armed groups in an effort to counter terrorism, narcotics trafficking and human rights abuses, among other reasons. When a group or country is sanctioned, their assets subject to U.S. jurisdiction are frozen. All transactions with them are prohibited, including transactions by FIs or NPOs.[28] The Treasury Department administers sanctions programs, and its Office of Foreign Assets Control (OFAC) can issue licenses that permit otherwise-banned transactions. Sanctions add to the compliance burdens on banks and NPOs and can have a compounding effect to AML/CFT requirements. In addition, the criminal prohibition against providing material support to Foreign Terrorist Organizations has been incorporated into the sanctions regime through Executive Order (EO) 13224. Although this report discusses some problems associated with U.S. sanctions, the primary focus is on AML/CFT regulatory requirements as a primary driver of derisking.

---

24 In 2015, SWIFT facilitated the exchange of an average of over 15 million messages per day, compared to an average of 2.4 million daily messages in 1995.

25 Bank for International Settlements, Committee on Payments and Market Infrastructures, "Correspondent Banking," July 2016, http://www.bis.org/cpmi/publ/d147.pdf.

26 Financial Stability Board, "FSB publishes progress report to G20 on action plan to assess and address the decline in correspondent banking," August 25, 2016, http://www.fsb.org/2016/08/fsb-publishes-progress-report-to-g20-on-actions-to-address-correspondent-banking-declines/.

27 David Artingstall, Nick Dove, John Howell, and Michael Levi, *Drivers & Impacts of Derisking: A Study of Representative Views and Data in the UK,* by John Howell & Co. Ltd. For the Financial Conduct Authority, February 2016, https://www.fca.org.uk/publication/research/drivers-impacts-of-derisking.pdf.

28 Limited exemptions apply. 50 U.S.C. § 1702(b).

The Risk-Based Approach

Although the letter of sanctions law imposes "strict liability" for violations,[29] international standards have been moving toward a more flexible RBA for nearly a decade. The FATF, the intergovernmental body that sets global standards to combat money laundering and terrorist financing, is the primary driver of this trend. Originally established in 1989 to address money laundering, FATF added terrorist financing to its agenda after 9/11 by adopting nine Special Recommendations, including Special Recommendation VIII on Nonprofit Organizations.[30] In the 2012 revisions of the FATF Recommendations, Special Recommendation VIII became Recommendation 8 (R8), and Recommendation 1, a new recommendation calling for a risk-based approach to implementation, was added. FATF evaluates and rates countries' implementation of all 40 of its standards.

FATF first introduced the RBA in 2007 to help ensure that measures to prevent money laundering and terrorist financing threats are commensurate to the risks identified. Previous approaches resulted in a "check the box" method of paper compliance rather than focusing on effective means to combat ML/TF. The intention of the RBA was clear: to create a more pragmatic, flexible and rational approach in which the focus shifted to address actual risks through controls based on customers and the precise risks they posed. A series of guidance documents described how various sectors, including FIs and governments, could implement the RBA.[31]

Overall, the RBA moved the international standard away from an emphasis on technical compliance in favor of regulation that is effective.[32] However, implementation of the RBA is an evolving process, as all stakeholders, including governments, NPOs and FIs, find ways of adjusting to these new methods. In the U.S., the legal framework governing sanctions and AML/CFT has changed little since 9/11 (see below) and does not adequately reflect the RBA set forth by FATF.[33] Although U.S. officials have articulated support for the RBA as policy, it is not a legal standard.[34]

---

29 50 U.S.C. § 1705; Financial Action Task Force & Asia/Pacific Group on Money Laundering, "United States Mutual Evaluation: Anti-Money Laundering and Counter-Terrorist Financing Measures," at 88, December 2016, http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

30 Financial Action Task Force, "FATF IX Special Recommendations 3," October 2001, http://www.fatf-gafi.org/media/fatf/documents/reports/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.

31 See Financial Access Task Force, "Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement," October 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf; Financial Access Task Force, "Guidance for a Risk-Based Approach: The Banking Sector," October 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf.

32 Neil Jeans, "Risk-Based Approach to KYC: Sound Concept, Complex Reality," https://risk.thomsonreuters.com/content/dam/openweb/documents/pdf/risk/white-paper/risk-based-approach-kyc-white-paper.pdf.

33 The FATF Mutual Evaluation Report of the U.S. notes that, "The obligation of FIs to implement T[errorist] F[inancing]-related S[sanctions] is an absolute strict liability one." United States Mutual Evaluation at 105.

34 Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214. See material support provision at "Providing Material Support to Terrorists," 18 U.S.C. § 2339B and the International Emergency Economic Powers Act Title II of Pub.L. 95–223, 91 Stat. 1626 See 50 USC 1701 et. seq.

Under the RBA, each FI undertakes its own internal risk assessment, tailoring its ML/TF threat-management program to its clients in order to manage risk effectively. This is a complicated and resource-intensive task because more work is required at the front end: FIs are expected to understand and assess specific risks and adopt policies to address them. This resulted in varying interpretations by FIs, leading to confusion within the industry.

In theory, the more flexible RBA approach would find that if FIs undertake appropriate processes to identify risk and adopt policies to mitigate them, they would be in compliance with regulatory requirements. In practice, however, banks have struggled to implement the RBA and have experienced significant variation and subjective determinations from federal regulators. According to a report by the British Bankers Association (BBA) and other organizations, "As regulatory views may differ from examiner to examiner, regulator to regulator and country to country, the avoidance of regulatory risk requires a broad 'safety buffer' to stay within expectations. With an increasing number of international banks under regulatory and legal actions (e.g. Deferred Prosecution Agreements, or Cease and Desist Orders etc.), the senior management of banks are developing a near zero tolerance for such regulatory risk."[35]

This complexity of the RBA was noted by the Comptroller of the Currency in 2016 when he said, "Banks must choose whether to enter into or maintain business relationships based on their unique business objectives, careful evaluation of the risks associated with particular products or services, evaluation of customers' expected and actual activity, and an assessment of banks' ability to manage those risks effectively. That's no easy task, given the complex environment in which banks operate. Multiple financial regulatory, law enforcement, and other agencies are involved in almost every situation."[36]

When FATF first established Special Recommendation VIII in 2001, it incorporated the notion that NPOs are "particularly vulnerable" to terrorist abuse (see Box). Over time, this view was considered to be inconsistent with the RBA and findings on the main sources of terrorist financing.[37] In June 2016, FATF removed the "particularly vulnerable" language, putting in its place a recommendation for a risk-based approach that is proportionate and avoids disrupting the activities of legitimate NPOs.

38

35 FATF Plenary and associated working groups, "De-risking: Global Impact and Unintended Consequences for Exclusion and Stability," at 7, October 2014, https://classic.regonline.com/custImages/340000/341739/G24%20AFI/G24_2015/De-risking_Report.pdf.

36 *Remarks by Thomas J. Curry, Comptroller of the Currency, Before the Association of Certified Anti-Money Laundering Specialists 15th Annual Anti-Money Laundering and Financial Crime Conference*, September 28, 2016, https://www.occ.treas.gov/news-issuances/speeches/2016/pub-speech-2016-117.pdf.

37 Emile van der Does de Willebois, "Nonprofit Organizations and the Combatting of Terrorism Financing: A Proportionate Response," 2010, https://openknowledge.worldbank.org/handle/10986/5926.

FATF TREATMENT OF NPOs [38]

In October 2001, FATF made protection of the NPO sector from terrorist abuse a critical component of the global fight against terrorism and a necessary step to preserve the integrity of NPOs. In approving Special Recommendation VIII (SRVIII): Nonprofit Organizations, FATF stated that NPOs were "particularly vulnerable" to terrorist financing abuse. It said countries "should ensure that they [NPOs] cannot be misused: by terrorist organizations posing as legitimate entities; to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset-freezing measures); and to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations."

FATF's Interpretative Note to SRVIII encouraged countries to focus on supervision and monitoring of the NPO sector and information-gathering and investigation. It cited vulnerabilities to abuse by terrorists as stemming from NPOs enjoying the public trust, having access to considerable sources of funds, being cash-intensive, having a global presence, and often being subject to minimal governmental oversight or background checks (e.g., registration, reporting, monitoring).

Over time, and with the introduction of the revised FATF 40 Recommendations in 2012 (SRVIII became R8), the FATF refined its guidance, acknowledging that "in the 12 years since the text of Recommendation 8 was first drafted, the threat environment and the NPO sector itself have continued to evolve." Recognizing that the NPO community had responded by developing standards and initiatives to help individual organizations ensure accountability and transparency in their operations, FATF moved toward targeted intervention, in part responding to NPO concerns about disproportionate impact of TF measures on legitimate activities.

In its 2014 Typologies Report and the 2015 Best Practices Paper on Combatting the Abuse of the NPOs, FATF explicitly noted that legitimate charitable activities should not be disrupted or discouraged and clarified the subset of NPOs that should be subject to greater attention: NPOs "engaged in 'service' activities" and operating "in a close proximity to an active terrorist threat." Additionally, emphasis was placed on having a flexible national terrorist financing approach and on "the application of effective, proportionate and dissuasive sanctions."

Reflecting changed realities concerning NPOs, FATF in June 2016 revised R8 and its Interpretive Note, directing countries to undertake a risk-based approach when considering counter-terrorism financing measures. Incorporating input from NPOs and the private sector through a stakeholder process, FATF recognized that not all NPOs should be subject to the same measures, especially "where humanitarian needs are acute and where charitable work contributes positively to the fight against regional and global terrorism."

38 Based on FATF reports and documents, including: FATF IX Special Recommendations (October 2001), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (February 2012), Risk of Terrorist Abuse in Non-Profit Organisations (2014), Best Practices: Combating the Abuse of Non-Profit Organizations (Recommendation 8) (June 2015), and Outcomes of the Plenary meeting of the FATF, Busan Korea, 22–24 (June 2016). http://www.fatf-gafi.org/publications/?hf=10&b=0&q=NPOs&s=desc(fatf_releasedate).

The AML/CFT Regulatory Environment

The legal and regulatory environment changed for both FIs and NPOs after 9/11. This section describes the legal, supervisory and enforcement context within which financial access problems have emerged.

For Financial Institutions

For more than 45 years, the Bank Secrecy Act has been a cornerstone of U.S. AML policies, anchoring the broad initiative to curb abuse of FIs. In October 2001, Congress passed the USA PATRIOT Act amending the BSA to, among other things, protect the U.S. and international financial system against the threat of terrorism through powerful new authorities to counter the financing of terrorism. To better protect the gateway to the financial system—correspondent accounts—Title III of the Patriot Act imposed new requirements on U.S. FIs to restrict certain types of foreign accounts, implement minimum due diligence and record keeping procedures, verify customer identification and beneficial ownership and adhere to U.S. sanctions.[39] The purpose was to deter the use of financial institutions by terrorist financiers and money launderers and to assist law enforcement efforts through the creation of an audit trail to identify and track terrorist suspects through financial transactions.

Working through FATF, the U.S. government led a global initiative that shifted FATF's focus from identifying and reporting suspicious activity to a much broader mandate of protecting the international financial system from the threat of financial crime through prevention. The language of financial crime prevention addresses both money laundering and terrorist financing, which includes identifying and reporting the proceeds arising from criminal behavior, preventing criminal and corrupt proceeds from entering the financial system and applying economic sanctions to prohibited countries or persons.[40] These new policies became essential elements of the Bush Administration's strategy to use American economic power to promote U.S. security through private sector action.[41] FIs became part of the long arm of American law enforcement as they began playing a new role as the first line of defense against terrorism financing. New agencies were created within the Treasury Department (such as the Office of Terrorism and Financial Intelligence), and significant new resources were allocated to fight illicit finance.

For international financial institutions, these developments marked a seismic shift, with financial crime management becoming a key priority. The results of this shift were new comprehensive management and reporting systems, transaction monitoring and AML/CFT/sanctions screening, enhanced procedures and controls for high-risk situations and a significant investment of resources

39 For background, see Sue E. Eckert, "The US Regulatory Approach to Terrorist Financing," in *Countering the Financing of Terrorism* (Thomas J. Biersteker and Sue E. Eckert, ed., 2008). The U.S. Patriot Act, enacted on October 26, 2001, is an acronym for the "United and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism," PL 107-56.

40 British Bankers Association et al., "De-risking: Global Impact and Unintended Consequences for Exclusion and Stability, Balancing public policy objectives," October 2014, https://classic.regonline.com/custImages/340000/341739/G24%20AFI/G24_2015/De-risking_Report.pdf.

41 See *Juan Zarate, Treasury's War: The Unleashing of a New Era of Financial Warfare,* September 2013.

in compliance activities. Extensive new regulatory requirements changed the compliance and risk management landscape. While some observers raised questions at the time concerning the appropriate balance between preventing financial crime and safeguarding other foreign policy objectives (such as financial inclusion and economic development), for the most part, these sweeping regulatory measures were adopted with little debate and without consideration of potentially unintended consequences.[42]

As they have developed, AML/CFT measures constitute a complex system of regulatory requirements for FIs[43] that include: freezing transactions and assets, maintaining records and reporting high-risk transactions and suspicious activities; self-disclosures of cross-border movement of certain products (e.g., currency, monetary instruments) and financial accounts held in foreign jurisdictions; collection and verification of information on customers and beneficial owners and sharing of information with other financial institutions, regulatory authorities and law enforcement.[44] In the wake of the 2008 financial crisis, the Dodd-Frank Act in 2010 further amended the BSA with increased regulatory obligations for FIs and other regulated entities.[45]

For FIs operating internationally, complying with differing legal and regulatory frameworks across national borders presents significant challenges. While the FATF as the global standard-setter has helped to somewhat harmonize AML/CFT requirements at the international level, within the U.S. alone there is a broad array of regulatory and policy agencies involved in AML/CFT issues.[46]

For Nonprofit Organizations

After the 9/11 attacks, the Bush Administration adopted a narrative of charities as "significant source of funds" for terrorist financing.[47] In the following years, greater information on terrorist financing threats and a more nuanced and evidence-based view emerged. Most examples of terrorist's abuse of charities involved non-U.S. organizations. The 9/11 Commission's Staff Monograph[48] found that extensive investigation "revealed no substantial source of domestic financial support" for the 9/11 attacks. A 2009 report from the UN Counter-Terrorism Implementation Task Force (CTITF) and the World Bank recognized growing concern for the

42 British Bankers Association et al., "De-risking."

43 The Patriot Act also expanded the range of institutions subject to BSA requirements to encompass all financial institutions, including money transmitters, security brokers/dealers, insurance companies and currency exchangers.

44 For an overview of the U.S. AML/CFT regime, see Protiviti, "Guide to U.S. Anti-Money Laundering Requirements: Frequently Asked Questions," November 2014, https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf.

45 The Wall Street Reform and Consumer Protection Act (Dodd-Frank Act, P.L. 111-203).

46 See Edward V. Murphy, "Who Regulates Whom and How? An Overview of U.S. Financial Regulatory Policy for Banking and Securities Markets," Congressional Research Service, January 30, 2015, https://fas.org/sgp/crs/misc/R43087.pdf.

47 *The Role of Charities and NGO's in the Financing of Terrorist Activities: Hearing Before the Subcommittee on International Trade & Finance of the Senate Committee on Banking, Housing, and Urban Affairs,* 107th Cong. (2002) (statement of Kenneth W. Dam, Deputy Secretary, U.S. Department of Treasury), https://www.gpo.gov/fdsys/pkg/CHRG-107shrg89957/html/CHRG-107shrg89957.htm.

48 John Roth, Douglas Greenberg, and Serena Wille, Staff Report to the Commission, "National Commission on Terrorist Attacks upon the United States: Monograph on Terrorist Financing" at 3, 2004, http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.

overemphasis on NPOs, cautioning, "States should avoid rhetoric that ties NPOs to terrorism financing in general terms because it overstates the threat and unduly damages the NPO sector as a whole." [49]

FATF Evaluation of U.S. – Recommendation on NPOs

In its 2016 Mutual Evaluation of the U.S., FATF noted that, "Striking the right balance and avoiding the disruption of legitimate NPOs activities can be challenging, particularly in high-risk conflict zones. As violations of T[errorist] F[inancing]-related S[anctions] are strict liability offenses, the authorities should continue to work with the NPO community to understand and mitigate the real TF risks that exist, while engaging stakeholders on banking challenges that some NPOs face while working in conflict zones." [53]

In 2015, the Department of Treasury issued a National Terrorist Financing Risk Assessment,[50] which discussed criminal enterprise and kidnapping for ransom as major sources of terrorist financing. While noting that "some charitable organizations, particularly those based or operating in high-risk jurisdictions, continue to be vulnerable to abuse for TF," the National Terrorist Financing Risk Assessment references sham or front organizations as the greatest threat to the nonprofit sector, rather than legitimate NPOs. The report stated, "there has been a shift in recent years towards individuals with no connections to a charitable organization recognized by the U.S. government soliciting funds under the auspices of charity for a variety of terrorist groups…"[51]

Many features of U.S. legal and regulatory policy, however, continue to reflect the outdated view of terrorist financing risks associated with the nonprofit sector. The original Special Recommendation VIII became embedded in various policies in the U.S. and around the world, and, as a result, the misperception that NPOs are "particularly vulnerable" still lingers today, resulting in constraints on the activities of legitimate NPOs.[52]

U.S. Regulatory Agencies

FIs and NPOs are both subject to complex regulatory systems that supervise them and enforce legal standards. This section describes the agencies involved in regulating FIs and NPOs and the scope of their oversight.

---

49 Counter-Terrorism Implementation Task Force, "Tackling the Financing of Terrorism," at 17, October 2009, http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_financing_eng_final.pdf.

50 Department of Treasury, "National Terrorist Financing Risk Assessment 2015," at 11, 2015, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

51 Ibid., at 43.

52 See Ben Hayes, Transnational Institute/Statewatch, "Counterterrorism, 'Policy Laundering' and the FATF: Legalising Surveillance, Regulating Civil Society," February 2012, https://www.tni.org/en/publication/counter-terrorism-policy-laundering-and-the-fatf.

53 U.S Mutual Evaluation, December 2016.

Regulatory Authorities for Financial Institutions

The U.S. regulatory and supervisory structure for FIs is complex, and FIs must deal with multiple government agencies. Generally, the government entity that grants the charter establishing an FI will be its primary regulator. A state bank is a bank chartered by the state in which it is located, and it usually offers only retail and commercial services. A national bank is a bank chartered and supervised by the OCC, pursuant to the National Bank Act. For the purposes of this report, the supervisory and examination functions of the agencies are most relevant (see Table 1).[54]

Table 1: Primary Regulators for U.S. Financial Institutions

<table>
<tr><th colspan="3">Primary Regulators Based on Chartering Authority</th></tr>
<tr><td colspan="2">For State Banks</td><td>For National Banks</td></tr>
<tr><td>Member of Federal Reserve</td><td>Non-member of Federal Reserve</td><td rowspan="2">Office of the Comptroller of the Currency</td></tr>
<tr><td>State and Federal Reserve</td><td>State and FDIC</td></tr>
<tr><td>FinCEN</td><td>FinCEN</td><td>FinCEN</td></tr>
</table>

The Office of the Comptroller of the Currency (OCC) regulates and supervises all national banks, in addition to monitoring federally chartered thrift institutions and the federal branches and agencies of foreign banks. The OCC conducts periodic examinations of national banks.

The Federal Deposit Insurance Corporation (FDIC) has broad statutory responsibilities that extend from insured depository institutions to bank holding companies (with more than $50 billion in assets). The FDIC further insures state-chartered banks that are not members of the Federal Reserve system. It conducts supervisory activities to determine an FI's compliance management system through three channels: compliance examinations, site visits and investigations.

The Federal Reserve is the U.S. central bank. It sets monetary policy, supervises and regulates financial institutions, promotes financial stability and consumer protection and works to promote a safe system for U.S. dollar transactions. It regulates state banks that are within its membership. The Financial Crimes Enforcement Network (FinCEN) is the primary AML/CFT regulator. It also supports law enforcement functions, provides financial intelligence to interagency and international efforts, issues and enforces regulations and collects and analyzes data that FIs are required to submit under the BSA filings, such as Suspicious Activity Reports (SARs).[55]

54 Regulators generally promote safety and soundness of banking operations, as well as other areas subject to state or federal regulation, including compliance with fair lending, consumer protection and other applicable statutes and regulations. While federal regulators encourage a risk-based approach, it is not enforced.

55 Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, *Suspicious Activity Reporting – Overview*, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_015.htm.

In addition to federal regulators, state governments have their own agencies that administer state banking laws, further adding to the complexity FIs face in dealing with regulatory requirements. Some, such as the New York Department of Financial Services, have been particularly active on AML/CFT issues, proposing regulations that extend personal liability for violations to individual compliance officers and senior managers within banks.[56]

Regulation of U.S. Nonprofit Organizations

The U.S. system for regulating nonprofit organizations is split among federal, state and local governments. Most NPOs are incorporated and registered under state law, and state/local laws often regulate fundraising practices to protect the public from fraud. At the federal level, regulation is focused on tax-exempt status and is administered by the IRS. Public charities and private foundations, exempt under IRS Section 501(c)(3), make up the largest of over two dozen categories of nonprofit organizations recognized by the IRS.[57] These are the only categories that can provide donors with tax deductions for their contributions.

Public charities are required to file annual informational reports with the IRS, and most states require some form of reporting as well. IRS Form 990 includes information on governance, finances and activities that must be available to the public. (Some organizations, such as houses of worship, are not required to apply for exempt status with the IRS or file annual information reports, but they may be required to register and make annual filings with state authorities to comply with state and/or local fundraising requirements.)

NPOs must also comply with laws directed at national security and sanctions that apply to all U.S. persons and entities. The exemptions for humanitarian assistance are limited. The material support prohibition only exempts medicine and religious materials.[58] The sanctions statute bars the U.S. President from blocking donations of "food, clothing and medicine intended to be used to relieve human suffering," unless he/she determines that such aid would "seriously impair his ability to deal with any national emergency."[59] This authority was invoked in EO 13224 on September 24, 2001. It has become routine practice for EOs to annually invoke this revocation of the humanitarian exemption and then grant case-specific licenses in each sanctions program.[60]

---

56 There has been increasing focus on personal liability of bank officers for compliance violations, with the Haider Moneygram case being a good example, among others. While previously possible, it was often easier for regulators to pursue firms, but regulators themselves have been criticized for failing to discipline senior individuals for failings that contributed to the financial crisis. Greater personal liability is becoming a reality in many jurisdictions, and a Thomson Reuters survey reports that 60% of respondents expect the personal liability of compliance officers to increase in the next 12 months, with 16% expecting a significant increase. Todd Ehret, Thomson Reuters Regulatory Intelligence, "Top Ten Concerns for U.S. Compliance Officers in 2016," 2016, http://info.accelus.thomsonreuters.com/Top10ConcernsUSComplianceOfficers.

57 Urban Institute, *The Nonprofit Sector in Brief 2015,* October 2015*,* http://www.urban.org/sites/default/files/alfresco/publication-pdfs/2000497-The-Nonprofit-Sector-in-Brief-2015-Public-Charities-Giving-and-Volunteering.pdf; IRS, Types of Tax-Exempt Organizations, https://www.irs.gov/charities-non-profits/types-of-tax-exempt-organizations.

58 18 U.S.C. § 2339A(b)(1).

59 50 U.S.C. § 1702(b)(2).

60 Charity & Security Network, "Safeguarding Humanitarianism in Armed Conflict," June 2012, http://www.charityandsecurity.org/sites/default/files/Safeguarding%20Humanitarianism%20Final.pdf.

NPOs AND DUE DILIGENCE

Robust due-diligence procedures by NPOs serve to protect the organization, its donors, programs, partners and recipients, as well as to prevent abuse from terrorists and criminals. The IRS and state regulators oversee public charities and private foundations, requiring financial, governance and activity reporting to assure appropriate stewardship of donor funds. In addition, the nonprofit sector provides a host of resources to help NPOs with governance and transparency, financial and program management, program implementation and more.

Because of the diversity of the nonprofit sector, there is no one-size-fits-all approach to due diligence, and most employ a variety of methods to implement measures appropriate to the range of activities in which they engage. Risk assessment by legitimate NPOs takes a variety of forms, depending on many variables. These include geographic location, type of activity and the history of engagement in the area. The NPO sector has undertaken significant efforts to develop more robust due-diligence procedures since 9/11. The FATF has said, "The NPO sector has responded considerably to these demands by developing several different standards and initiatives to help individual organisations ensure accountability and transparency in their operations."[61]

Examples of NPO due-diligence resources and programs include the following.

1. The 2005 "**Principles of International Charity"**[62] includes measures for fiscal responsibility on the part of organizations providing resources to international programs:

   a. in advance of payment, determining that the potential recipient of monetary or in-kind contributions has the ability to both accomplish the charitable purpose of the grant and protect the resources from diversion to non-charitable purposes;

   b. reducing the terms of the grant to a written agreement signed by both the charitable resource provider and the recipient;

   c. engaging in ongoing monitoring of the recipient and of activities under the grant; and

   d. seeking correction of any misuse of resources on the part of the recipient.

2. MercyCorps[63] has developed a **Due Diligence Assessment Tool** to manage possible risks that includes questions to evaluate potential clients, review existing relationships before committing to additional projects/assistance, understand existing risks and incorporate corresponding mitigation activities, and discover emerging risks.

3. At a global level, the **Sphere Project**, composed of representatives of various humanitarian agencies, introduced common principles and "universal minimum standards in life-saving areas of humanitarian response."[64]
(See *Table 9: Transparency Standards and Initiatives Developed by NPO Sector*, Chapter 7)

61 *Financial Action Task Force Risk of Terrorist Abuse of Nonprofit Organizations*, at 22, http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf.

62 Council on Foundations and Treasury Guidelines Working Group of Charitable Sector Organizations and Advisors, "Principles of International Charity," March 2005, at http://www.foreffectivegov.org/sites/default/files/npa/Treasury%20Principles%20Final%20Document%20.pdf.

63 "Due Diligence Assessment Tool," Mercy Corps, https://d2zyf8ayvg1369.cloudfront.net/sites/default/files/Tool%204%20Due%20Diligence%20Assessment.pdf

64 http://www.sphereproject.org/about.

Enforcement

The Bank Examination Process

Since 9/11, U.S. agencies have intensified financial supervision and compliance examinations to ensure that the U.S. financial system is protected from ML/TF risks. Federal bank examinations are intended to set the terms for FIs' behavior regarding legal and enforcement compliance.

Because enforcers of the BSA have the ability to recommend civil fines,[65] bank examiners have significant influence on FI behavior. They participate in the assessment of financial institutions to determine the existence of unsafe and unsound practices, violations of law and regulation, the adequacy of internal controls/procedures and the general character of management.[66] Examinations are detail-intensive, covering a broad range of procedures and practices, from staff knowledge of emerging risks to management information systems. In particular, examination procedures assess whether bank controls offer reasonable protection from ML/FT risks, determine whether high-risk accounts are identified and monitored, and evaluate the adequacy of procedures to monitor and report suspicious activities.

Examiners' work is governed by the BSA/AML Examination Manual, which is produced by an interagency body.[67] It provides specific guidance for bank examiners to review FI compliance, including management of higher-risk customers. The Manual, last updated in 2014 and not due to be revised until 2018, includes a section on NPOs that does not reflect the June 2016 changes in FATF's R8. As such, it describes the entire sector as risky, stating, "the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists."[68] It goes on to require FIs to conduct extensive background investigations of NPO customers, including details on their governance, financial procedures, volunteer and donor base, program operations and associations. For nonprofits that work outside the U.S., it adds the following steps:

- Evaluating the principals
- Obtaining and reviewing the financial statements and audits
- Verifying the source and use of funds
- Evaluating large contributors or grantors of the NGO
- Conducting reference checks

65 Federal Deposit Insurance Corporation Regulations, Risk Management Manual of Examination Policies, Sec. 14.1-3, https://www.fdic.gov/regulations/safety/manual/section14-1.pdf; Office of the Comptroller of the Currency, Examinations: Overview, https://www.occ.gov/topics/examinations/examinations-overview/index-examinations-overview.html.

66 Federal Deposit Insurance Corporation, *What We Do: Supervise Banks and Ensure Compliance with Fair Credit and Community Reinvestment Statutes*, https://www.fdic.gov/about/jobs/do.html#be.

67 The FFIEC, an interagency body promoting uniformity in the examination and supervision of financial institutions, is comprised of the Board of Governors of the Federal Reserve System, FDIC, NCUA, OCC, CFPB, and OTS.

68 FFIEC, "Bank Secrecy Act Anti-Money Laundering Examination Manual Bank," at 311-312, https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2014.pdf.

As was previously mentioned, obtaining and evaluating this information is a resource-intensive process. The vagueness of some of the steps, such as how far an FI must investigate the volunteers and donors of an NPO, opens the door to inconsistent implementation. Moreover, extensive questioning by examiners of charity accounts signals to FIs that these accounts are problematic. Given the potential high cost of conducting this due diligence on NPO customers, it is not surprising that some FIs determine that it is not cost-effective to serve them.

Adopting practices to acquire concrete client information (known as "know your customer" [KYC] processes) can provide FIs with legitimate data, promoting informed and fair decisions when offering financial services. Indeed, data, rather than examiners' opinions, are supposed to drive a specific FI's risk-based approach to conducting business. However, "second-guessing" by examiners of individual transactions and differing interpretations of risk have sent confusing and mixed signals and have resulted in regulatory actions for "wrong" assessments of risk.[69]

Enforcement Trends for FIs

In recent years, regulators have cracked down on AML/CFT violations, imposing unprecedented fines, in part as a reaction to Congressional criticism of regulators for "showing too much deference to the banks" in the aftermath of the 2008 financial crises and investigation of HSBC money laundering activities.[70] The CGD report noted that over the last 15 years, both the number and value of AML-related fines have increased in both the U.S. and the UK.[71]

> ***The large number of enforcement actions, the unparalleled monetary fines and settlements and the severity of the terms have had a chilling effect throughout the financial sector.***

For example, in 2012, several U.S. regulatory agencies cooperated in a settlement that resulted in a $1.9 billion fine on HSBC for violating sanctions and laundering hundreds of millions of dollars related to Mexican drug trafficking. The same year, Standard Chartered Bank paid almost $1 billion to settle actions brought by the federal government and the New York State Department of Financial Services for moving millions of dollars through the financial system on behalf of sanctioned Iranian, Sudanese and Libyan entities.[72] In 2015, BNP Paribas received a sentence of 5 years' probation from a U.S. judge in connection with "a record $8.9 billion settlement resolving claims that it violated sanctions against Sudan, Cuba and Iran."[73] While announcing the settlement, then-U.S. Attorney General Eric Holder noted that he hoped the settlement would serve as a warning to other firms that did business with the U.S. that "illegal

69 Staci Warden, "Framing the Issues: De-Risking and Its consequences for Global Commerce and the Financial System," *Center for Financial Markets*, at 4, July 2015, http://www.milkeninstitute.org/publications/view/727.

70 Nathaniel Popper, "Regulators and HSBC Faulted in Report on Money Laundering," New York Times Deal Book, July 16, 2012, http://dealbook.nytimes.com/2012/07/16/scathing-report-details-money-laundering-problems-at-hsbc/?_r=0.

71 *Unintended Consequences of Anti-Money Laundering Policies for Poor Countries*, Center for Global Development ("CGD Study"), at 11, November 9, 2015, http://www.cgdev.org/publication/unintended-consequences-anti-money-laundering-policies-poor-countries.

72 Gavin Finch and Edward Robinson, "Why Banks Like HSBC Won't Send Money to War-Zone Charities," Bloomberg, May 11, 2016, https://www.bloomberg.com/news/articles/2016-05-11/banks-cutting-money-flow-for-charities-squeezes-relief-in-syria

73 Nate Raymond, "BNP Paribas sentenced in $8.9 billion accord over sanctions violations," Reuters, May 1, 2015, http://www.reuters.com/article/us-bnp-paribas-settlement-sentencing-idUSKBN0NM41K20150501.

conduct will simply not be tolerated."[74] The large number of enforcement actions, the unparalleled monetary fines and settlements and the severity of the terms have had a chilling effect throughout the financial sector. It should be noted that most criminal investigations do not end with fines on FIs, but having to defend such an investigation can be extraordinarily expensive.

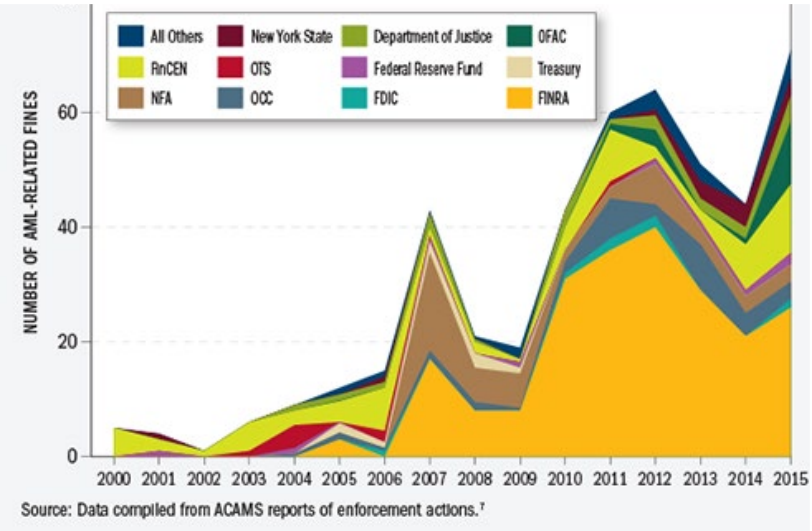
Enforcement Trends for NPOs

Between late 2001 and early 2009, the Treasury Department designated nine U.S. charities as supporters of terrorism, using the expanded powers derived from the Patriot Act. Seven of these NPOs were Muslim charities. These designations effectively prohibited any transactions with these organizations and froze their funds.

In the ensuing years, litigation on the constitutionality of the Treasury Department's administrative appeal process has produced mixed results. The most recent court decisions found the process to be unconstitutional in that it denied due process by not giving the NPOs a meaningful opportunity to contest their designation and seized (froze) their funds without a warrant.[75]

Since 2009, the focus of enforcement has shifted to criminal prosecutions of "individuals supporting various terrorist groups seeking to raise funds in the U.S. under the auspices of charitable giving, but outside of any charitable organization recognized as tax-exempt by the U.S. government."[76] When asked in a 2016 Congressional hearing why no U.S. charities have been shut down since 2009, then-Assistant Secretary for Terrorist Financing Daniel Glaser noted that the Treasury's engagement with NPOs has "reduced the opportunity for [charities] to be abused" by terrorist organizations. He also noted the trend of fraudulent fundraising by sham organizations.[77]

Figure 2: Number of AML-Related Fines by U.S. Regulators 2000-2015*



***Source: Unintended Consequences of AML Policies (Data compiled from ACAMS reports of enforcement actions)** https://www.theclearinghouse.org/publications/2016/2016-q3-banking-perspectives/aml-unintended-consequences

74 Nathaniel Popper, "Regulators and HSBC Faulted in Report on Money Laundering," New York Times Deal Book, July 16, 2012, http://dealbook.nytimes.com/2012/07/16/scathing-report-details-money-laundering-problems-at-hsbc/?_r=0.

75 Kay Guinane and Cherie L. Evans, "Gap Between Tax and Sanctions Law Blocks Lifesaving Aid," Tax Notes, October 10, 2016; Al Haramain Islamic Foundation Inc. v. Treasury, 686 F.3d 965 (9th Cir. 2012) and KindHearts for Charitable and Humanitarian Development, Inc. v. Geithner, 710 F. Supp. 2d 637 (N.D. Ohio 2010).

76 U.S. Mutual Evaluation, December 2016.

77 "Stopping the Money Flow: War on Terror Finance, Joint Hearing Before Subcommittees of House Committees on Foreign Affairs and Armed Services," Questions for the Record for Assistant Secretary Daniel Glaser, June 9, 2016.