Anti-Terrorist Financing Risk Management: Protecting Your Organization’s Reputation through Know-Your-Grantee Efforts

Keep risk from exploiting your good cause and stay focused on mission-critical efforts.
Executive Summary

LexisNexis® recommends charitable organizations consider adopting best practices published by global organizations and government agencies in order to preserve public trust. Mitigating the risk of reputational damage is critical to charitable organizations. One of the best ways to prevent becoming involved in terrorist activities is to truly know the persons with whom you choose to conduct business. Know-Your-Grantee programs require resources, and that is something that nonprofit organizations typically lack. There are several lessons from the regulated banking industry that can be applied in the non-profit sector. A risk-based approach allows organizations to focus resources where they matter most. Software tools can help increase the efficiency of Know-Your-Grantee efforts through automation, helping your personnel to concentrate on the important work of helping those in need.

Introduction to risk management

The overall effort required to manage risk can be easier and more manageable than one might expect. Tools are available to help automate due diligence steps, and best practices exist to help organizations tailor their efforts to their unique situations.

Managing risk, any type of risk, classically involves two steps. The first is considering the severity of the consequences should an event take place. The second is considering the likelihood of the event occurring in the first place.

Consequences

When it comes to the risk of being involved, even unwittingly, in terrorist financing, the consequences can be serious. The problem of charities being exploited by terrorism financiers is very real. In fact, the U.S. Treasury’s Office of Foreign Assets Control (OFAC) maintains a site dedicated to the key issues regarding protecting charitable organizations. “To date, the United States has designated forty-three charities worldwide and twenty-nine associated individuals for their support of terrorist organizations and operations. These seventy-two charities and individuals comprise over fifteen percent of all U.S.-designated terrorist supporters or financiers, indicating the primary importance of charities as a critical means of support for terrorist organizations and activities.”

It is important to understand that the risk is not limited to the distribution of charitable funds to individuals who support acts of terrorism. It goes beyond the diversion of funds. “Terrorist abuse also includes the exploitation of charitable services and activities to radicalize vulnerable populations and cultivate support for terrorist organizations and activities. As reported through a wide range of media sources, terrorist organizations deliberately establish, infiltrate or otherwise exploit charitable organizations to build terrorist support networks.”

Likelihood

As risk managers ask themselves “What are the chances of being used as a conduit for terrorist financing?,” they sometimes determine that the possibility is extremely remote. Naturally, they question the wisdom of committing significant resources to manage the risk. Some non-profit organizations have voiced the concern that their resources are already tight. Spending more on administrative tasks like terrorist list checking leaves less to spend on true charitable initiatives, such as addressing poverty or providing humanitarian aid.

This resource dilemma is not limited to the world of not-for-profit organizations. Many financial institutions struggle to define the level of effort that results in a compliance program that is appropriate to the risks they face. Yet that is exactly what is required by regulation in the banking and finance industry. These requirements have been in place for some time, and there are parallels that can be made to the non-profit sector.
Lessons learned from financial services

The first lesson is that the perception of being involved—whether or not those perceptions are true—can be detrimental. Imagine your organization’s name on the front page of a major national newspaper with headlines that include the words “suspicion” and “terrorist financing.” It is quite likely that at least some of your contributors will disassociate themselves, potentially impacting your funding. While the chances may be remote, the consequence is potentially grave. Protecting the reputation of a charitable organization is critical to its survival, so most of us would agree that some level of effort is worthwhile.

Another lesson is the wisdom in taking a risk-based approach. The idea is to focus your resources on the areas where you actually identify potential risk. What does this look like in the banking world? An example might be the questions that are asked during an account opening process. Certain questions are standard, but in some situations where the bank faces more risk (i.e., international transactions), the customer service personnel may be instructed to ask supplemental questions, or run background checks. A risk-based approach helps ensure that organizations do not waste time and money on efforts that will not provide a return on their investment.

With resources already limited, this concept fits non-profit organizations. This lesson finds its way into recommendations included in the U.S. Department of the Treasury’s Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities (Guidelines): “…charities should apply a risk-based approach, particularly with respect to engagement with foreign grantees due to the increased risks associated with overseas charitable activity.”

A third lesson is that the cornerstone of protecting yourself from unwittingly becoming a party to terrorist financing or anti-money laundering schemes is understanding—truly knowing—the people with whom you choose to conduct business. The Guidelines echo this, with recommendations that suggest a charity’s vetting practices should include due diligence efforts, including “a reasonable search of publicly available information” to determine whether any of its grantees is suspected of activity relating to terrorism, including terrorist financing or other support.

Know-your-grantee programs

This third lesson above presupposes that you have gathered information from your grantee in order to be able to compare it to lists of suspected terrorists. Many non-profit organizations already gather such information, and some already conduct research about donors or grantees on their own. Collectively we call these “Know-Your-Grantee” efforts, which are very similar to Know-Your-Customer practices found in the banking arena. The focus of the Guidelines is on knowing your grantee, your donors and other business partners, and mirrors the banking industry’s Customer Identification Programs (CIP) requirements that resulted from the USA PATRIOT Act. While we note that the Guidelines are, so far, voluntary, we recommend that non-profits at least consider adopting some of the recommendations.

Why is compliance with the Guidelines sound business for non-profits? Why is dedicating resources to an Anti-Terrorism Program a good idea? In an article in The Nonprofit Times, Joseph Bender points to the importance of essential elements contained within the Guidelines. Organizations want to ensure their grantee is capable of meeting their aims claimed in the grant application; ensure funds won’t be used for illegitimate or illegal use; have a documented agreement or contract between the grantee and the organization that clarifies precisely how funds will be implemented; and provide continual monitoring of the use of funds and even establish the possibility or right to conduct an audit.
In an Anti-Terrorism and Charity Law Alert, Carter and Associates state that the non-profit sector has been “identified as a ‘crucial weak point’ in anti-money laundering and terrorist financing initiatives of the international community... These initiatives have brought about a ‘new day’ for charities...”7 Checking against government watch lists to ensure persons are not affiliated or members of terrorist organizations is one way to protect the reputation of your organization.

In addition, if you are a U.S.-based charity, you are subject to OFAC regulations, and scanning against the OFAC lists is therefore prudent. In fact, “all U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches.”8

OFAC publishes a list of Specially Designated Nationals (SDNs); a list of Non-SDNs that currently addresses transactions with some members of the Palestinian Legislative Council; and an index of Sanctions Programs where compliance professionals can review specific requirements of jurisdictional or list-based sanctions programs. It is recommended that non-profit organizations ensure that their connections—internal and external—do not match entities on these lists.

Software tools are available

How feasible is it for a charitable or other non-profit organization to filter their connections through these “lists”? Quite honestly using a purely human effort would be excruciatingly time intensive and detrimental to the organization’s time available for other needed efforts. Content of the SDN list, not to mention other available terrorism lists recommended in the globe (Terrorism Exclusion List or European Union Terrorism List, for example) is extensive—housing more than 5,000 entities or records.

Compliance technology exists to reduce the time involved and increase the ability to make timely and accurate decisions. In fact, interdiction (list checking) technology is quite mature since it has been in place in the banking and finance industry for over a decade. What that means for non-profits considering a purchase is that they can expect to enjoy the benefits of competition: a variety of products, with a variety of features, all at a variety of prices. The expense required to implement a technology solution for this highly clerical and time intensive compliance task is frequently warranted. Financial institutions have already found that using the right solution will help increase efficiencies—freeing up your personnel to do other important tasks. After all, interdiction is suited to automation. You can reserve the most important decisions about watch list matches for the human effort, but for a fraction of what a salary costs, an organization is best attending to the Guidelines by implementing a software tool.

Policies, procedures and compliance technology tools can go a long way in meeting sound practices for ‘good business’ and protecting national security, but also preventing reputational risk or loss of ability to operate the organization. A drastic but possible consequence seen in the media is the loss of continued donor opportunities related to matches to government watch lists (discoveries of money laundering or terrorist financing evidence).9 Another possible consequence is criminal charges, as seen in this example included in Treasury’s Typologies and Open Source Reporting on Terrorist Abuse of Charitable Operations in Post Earthquake Pakistan and India:

“The Holy Land Foundation for Relief and Development (HLF), originally known as the Occupied Land Fund, was established in California in 1989 as a tax-exempt charity and relocated to Texas in 1992. It had offices in California, New Jersey and Illinois, and individual representatives spread throughout the United States, West Bank and Gaza. HLF provided millions of dollars of material and logistical support to HAMAS offices in the West Bank and Gaza and other charitable organizations that are part of HAMAS or controlled by HAMAS members. HLF and several of its directors were indicted on criminal charges in July 2004...”10
“Fiscal responsibility is fundamental to international charitable work. Therefore, an organization’s commitment to the charitable use of its assets must be reflected at every level of the organization.”

Summary

Knowing your grantees, grantors and other business partners within the world of non-profits and charitable organizations is fairly new, but it is compelling today with the final Guidelines issued by the U.S. Treasury in the fall of 2006. LexisNexis recommends that non-profit organizations consider implementing some, or all, of the recommendations in the Guidelines, or in other best practices published by international organizations. Program components with which to meet the optional Guidelines and to reduce risk, include a number of best practices recommendations plus the implementation of a technology solution to reduce resource in scanning grantors, grantees and other business partners against the OFAC SDN list and other terrorism watch lists.

Sources

1 OFAC’s site identifying key issues regarding protecting charitable organizations can be found at <http://www.treas.gov/offices/enforcement/keyissues/protecting/charities_exec-orders.shtml>
3 Ibid.
4 Ibid.
9 Carter, et al.

Additional sources

For more information:
Call 866.858.7246, visit lexisnexis.com/risk/financial-services

About LexisNexis Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.