THE WASHINGTON INSTITUTE for Near East Policy

PolicyWatch #1251 : Special Forum Report

U.S. Efforts against Terrorism Financing: A View from the Private Sector

Featuring Robert Werner
June 26, 2007

On June 15, 2007, Robert Werner addressed The Washington Institute's Policy Forum seminar series. Managing director of Merrill Lynch's Monetary and Financial Control Group since December 2006, he previously served as director of the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and, before that, as director of the department's Office of Foreign Assets Control (OFAC). The following is a rapporteur's summary of his remarks.

Now more than ever, the private sector needs to help prevent terrorism financing. Emerging markets in the Middle East, Africa, and Southeast Asia present law enforcement authorities and the private sector with new challenges and possibilities in the areas of terrorism financing and money laundering. For those companies that value their reputations and wish to uphold the moral and ethical imperative to prevent the funding of illicit activity, increased cooperation with U.S. government efforts is vital.

Background

Although terrorism financing and money laundering are often categorized together, the former is in fact much more difficult to detect. As opposed to laundering -- the process of layering and integrating funds into the financial system -- terrorism financing often involves clean money being used for illicit purposes. In addition, terror financiers transfer funds through increasingly sophisticated means. Beyond using traditional banks and wire transfers, they are now investing in securities and moving money through related transactions.

There is a misconception that terrorists do not require large sums of money to operate. Although the cost of individual attacks is relatively low, the cost to maintain terrorist infrastructure is comparatively high. The focus of efforts to counter terrorism financing should not be preventing individual attacks, but breaking the networks that facilitate them. Even this worthwhile effort can have unintended consequences, however. The offshoots of large, sophisticated terrorist networks remain highly dangerous even when they lack formal connections to said networks.

What the Private Sector Can Do

In the wake of the September 11 attacks, profiling was widely used in the private sector because of a lack of options and innovation. Against terrorism financing, however, profiling is both ethically questionable and ineffective, creating excessive false positives, producing superfluous information, and reducing analysts' likelihood of identifying suspicious transactions.

Instead, many financial institutions use the Treasury Department's list of specially designated nationals (SDNs). Such lists are valuable because they highlight relationships, sensitize people, and disrupt illegitimate activities -- but they are not a panacea. Once designated, banned entities change names quickly, so the initial designation may only have disruptive, not prohibitive effects. Similarly, terrorist organizations and regimes

that support them (e.g., Iran and Syria) often use innocuous-sounding front companies. Accordingly, both the U.S. government and private sectors need to rely on due diligence procedures to ensure that bad actors do not have access to money. Because financial institutions are not privy to much of the information underlying a designation, it is often difficult for them to determine whether to conduct business with a given actor, especially if only small branches of that organization are designated.

To report illicit activities, financial institutions are required to file suspicious activity reports (SARs). It is important that institutions report anything suspicious. Very few SARs actually relate directly to terrorism financing. More often, valuable SARs are drawn from suspected criminal activity or subpoenas.

The Role of the Patriot Act

In preparing reports on specific entities, financial institutions often rely on private companies with ties to government officials or with people on the ground intimately familiar with a given situation. But these reports are often unsourced, based on rumors, or simply incorrect. In response, institutions must come to their own best judgment on whether the risk of doing business with a specific entity outweighs the potential reward. A framework to counteract this shortcoming can be found in the USA PATRIOT Act, Sections 314(a) and 314(b). These sections deal with the exchange of information between the government and financial institutions, and among financial institutions, with regard to identifying money laundering or terrorist activity.

Based on past indications of success in other fields, Section 314(b) holds promise for enhancing information sharing between financial institutions. They already pool information relating to fraud, creating comprehensive "fraudnet" databases that serve as an excellent repository of available knowledge. Similar shared databases should be created for terrorism financing in order to inform financial institutions about dealing with certain actors.

That alone would not be sufficient, however, because financial institutions simply do not have enough information to make accurate judgments. Accordingly, section 314(a) mandates an iterative exchange of information related to terrorism financing and money laundering between the government and private sector. Unfortunately, apart from public designations and isolated individual cases, this exchange has not happened -- in part because of the need to protect sensitive sources and methods. Working groups composed of government and private sector officials should be developed and modeled on relationships between the Defense Department and its contractors. If appropriate, officials at financial institutions should receive security clearances to constructively participate in these discussions.

Lessons Learned

For the private sector, there are several important lessons to be learned from recent experience:

Don't view automated systems as panaceas. Transaction monitoring systems are useful, but illicit activity often resembles legitimate activity. In order to reliably detect suspicious activity, financial institutions should not underestimate the value of manual surveillance by analysts.

Develop and maintain relationships with regional law enforcement. When filing SARs, it is important to alert the appropriate authorities.

Avoid process burnout. Too often, staff members focus on just getting through the data rather than the overarching objective -- catching the bad guys.

Engage the business side in decisionmaking. Consultation between the compliance and business sides of financial institutions increases the latter's buy-in to the compliance process, particularly when the risk factors and concerns are explained.

Avoid pro forma training. Required training is usually done via the internet. It is important to supplement general training with in-person, targeted training, which results in more constructive participation and better understanding.

Maintain coordinated and consistent programs within a company. Financial institutions, especially large, multinational corporations, should encourage internal unity and consistency.

Understand your own products. The people working toward compliance need to be involved in the development and execution of relevant financial products.

Add personnel to areas that make a difference. Like other organizations, most financial institutions face the question of where to allocate their personnel. It is important to allocate scarce resources to those areas that give the most significant return in terms of an effective compliance program.

Most important, information sharing among financial institutions and the government needs to be improved. There needs to be a comprehensive institutional and cultural shift within the private sector. In general, passing suspicious accounts to competitors should not be seen as a competitive advantage.

Conclusion

Although significant progress needs to be made on information sharing, the legal framework to leverage these changes exists in the form of Sections 314(a) and 314(b) of the Patriot Act. These laws provide protection for financial institutions seeking to share information with the intent of countering terrorism financing or money laundering. In the past few years, the U.S. government has vastly improved its understanding of terrorism financing. For progress to continue, the private sector needs to be increasingly included as a significant partner in this process.

This rapporteur's summary was prepared by Jake Lipton.

Copyright 2008 The Washington Institute for Near East Policy