BANKS AND THE USA PATRIOT ACT

John J. Byrne

The American Bankers Association (ABA) supports the goal of the USA PATRIOT Act to curb terrorist financing and is particularly pleased that it extends to all financial institutions anti-money laundering requirements that previously applied only to banks. Implementing the law has revealed weaknesses, however, related to detecting those routine and often small transactions that terrorists typically have employed. The ABA advocates more sharing of intelligence about terrorists with the financial community.

John J. Byrne serves as director of the American Bankers Association's Center for Regulatory Compliance.

While the U.S. banking industry has a long history of supporting law enforcement in areas such as money laundering, Washington's efforts to curb terrorist financing through stricter banking rules are well intentioned but may miss the mark unless the government increases its commitment to provide banks with the intelligence they need.

The U.S. Congress responded to the tragic events of 9/11 by passing the 300-page law known as the USA PATRIOT Act. Acting in three weeks' time and with overwhelming bipartisan support, Congress clearly wished to enact useful and helpful legislation to address the scourge of terrorist financing. Most of the provisions, however, failed to address that particular crime.

Were these new laws necessary, or did we simply need more government intelligence? The post-9/11 briefings from law enforcement make it clear that, for the most part, the type of financial transactions that the hijackers utilized are not adequately addressed by the USA PATRIOT Act. The fact is that U.S. financial institutions, without additional government intelligence, cannot detect or prevent transactions related to terrorist financing.

This article will examine how the challenges facing the U.S. financial sector have changed since the passage of the USA PATRIOT Act in October 2001 and what else can be done to stop the flow of the financial resources to terrorists.

THE PATRIOT ACT

It is clear that the lion's share of the PATRIOT Act provisions addressing the financial industry (title III) were left over from previous unsuccessful legislative vehicles covering traditional money laundering. Despite lingering questions on how the law would be implemented and

whether it would effectively address terrorist financing, the American Bankers Association (ABA) actively supported the PATRIOT Act because it covered a myriad of new financial service providers that previously did not have anti-money laundering (AML) obligations, and it contained several other new provisions long advocated by the industry.

The key provisions of the act related to banking (and emphasized by the congressional committees responsible for authorship) include:

• making bulk cash smuggling a crime and requiring registration of black market underground financial networks

• modernizing anti-counterfeiting laws to prohibit U.S. financial institutions from providing financial services to foreign "shell" banks

• expanding public-private partnerships to help law enforcement identify, track, and stop terrorists' financial activities

• reporting "in real time" suspicious financial activity to law enforcement agencies

• requiring financial institutions to verify the identity of their new account holders, and

• requiring customers to provide financial institutions with truthful information when opening accounts

Most important to the banking industry was the provision that required all financial institutions to institute anti-money laundering compliance programs, a bank requirement since 1987.

What Changed For Banks?

As far as the practical effect of these new laws, most of the provisions simply expand obligations that were part of the AML regulatory oversight process. For example, there are provisions that require due diligence for private banking activities or correspondent bank relationships. The federal banking agencies must review and criticize banks that fail to cover those "risky" relationships with enhanced due diligence.

One of the new obligations under title III is section 326, which requires financial institutions to have account opening procedures or a "customer identification program." Banks and some covered financial institutions such as securities firms, mutual funds, and commodity futures traders (insurance companies are pending) have to obtain four pieces of information (name, address, date of birth, and government identifiers such as social security numbers) and attempt to verify that information. Because banks have been requesting identification of customers since the beginning of banking, this new obligation is a formalization of business as usual.

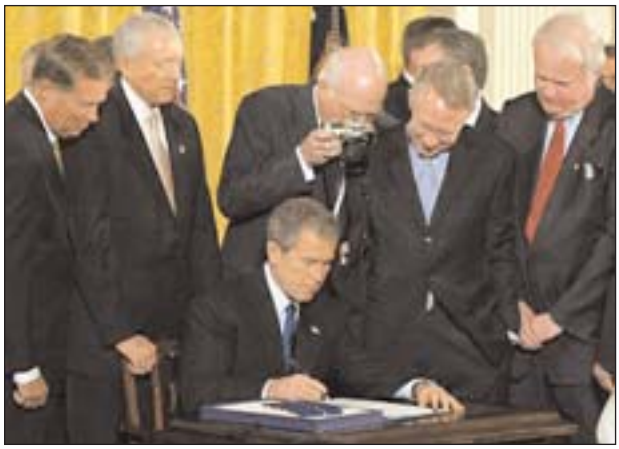
What do the changes mean for the international community?

What you may see is that a U.S. institution will want both a primary and a secondary form of identification of a potential foreign account holder. The problem with that approach is that, because many different forms of identification are unfamiliar to U.S. institutions, banks may be reluctant to open certain accounts. In addition, there are continuing issues with remote account openings since there are currently no public databases containing information to verify the identification of foreign individuals as there are for U.S. individuals. Therefore, in order to maintain relationships with U.S. financial institutions, potential foreign account holders will have to work closely with the institutions to ensure continued relationships.

PATRIOT Act Compliance

Given the increased attention to due diligence, what exactly do U.S. regulators expect banks to do to perform adequate compliance? One example is unless there is a finding by the secretary of the Treasury that certain jurisdictions cause money laundering concerns for the government, as was the case with areas such as Nauru, Ukraine, and Burma, the industry must look to other sources of information to determine whether there is a risk involved when dealing with certain jurisdictions.

One such source is the Financial Action Task Force (FATF) and its list of non-cooperative countries (NCCT). An NCCT designation means that the country had weak or non-existent laws regarding money laundering prevention. Since 2000 there have been 24 jurisdictions designated as non-cooperative. Since banks are required to carry out increased due diligence on these countries, it is important to stay abreast of these designations.



AP Photo/Doug Mills

President Bush signs the anti-terrorism bill into law during an October 2002 ceremony in the White House East Room.

It should be emphasized that financial institutions can still do business with an entity in a non-cooperative country, but they will be criticized for not spending more time reviewing the accounts in those institutions. So for a risk assessment to comply with the elements of this new law, regulators expect a bank to review publicly available information. The problem with this is that it really does not assist a bank in preventing terrorist financing.

Financial Profile of 9/11 Criminals

Our association was briefed by federal law enforcement officials on the various methods of how terrorists used the financial system prior to 9/11. One major theme should be clear: it does not cost much to rent a car, stay at a hotel, or buy a plane ticket. Therefore, terrorist financing transactions, by their very nature, are routine and are not the same as the elements of traditional money laundering.

The recently completed 9/11 Commission concluded "that the 9/11 attacks cost somewhere between $400,000 and $500,000 to execute." In addition, the 9/11 criminals' use of financial institutions was described as follows:

• Accounts were checking accounts of around $3,000.

• Applications indicated that the accountholders were "students."

• Identification used were visas issued by United Arab Emirates, Saudi Arabia, and Germany.

• Accounts were opened within 30 days of entering the country.

• Account holders checked their balances at ATMs several times a day.

According to the 9/11 Commission:

> The conspiracy made extensive use of banks in the United States, both branches of major international banks and smaller regional banks. All of the operatives opened accounts in their own names, using passports and other identification documents. There is no evidence that they ever used false social security numbers to open any bank accounts. Their transactions were unremarkable and essentially invisible amidst the billions of dollars flowing around the world every day.

In short, we believe that financial institutions could not have detected the 9/11 attackers' criminal activities without additional and specific government intelligence. Low dollar accounts cannot be effectively monitored, and creating a system to assess how often someone engages in a "transaction inquiry" at an ATM is not practical. In addition, since the identification utilized by the terrorists was not false, improved identification procedures that are required under the PATRIOT Act, while useful to prevent identity theft, would not have prevented access to a financial institution. We have learned some important lessons from the briefing mentioned above and ABA now recommends that banks not accept visas as a primary form of identification.

PATRIOT Act As Prevention Tool

One section of the USA PATRIOT Act that can address the amorphous concept of terrorist financing is Section 314(a). The 314 process requires financial institutions to search accounts for potential matches to names on government investigative lists. Under this provision:

• 314(a) requests are sent from the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) and batched and issued every two weeks, unless otherwise indicated in the request.

• After receiving a 314(a) request, financial institutions have two weeks to complete their searches and respond with any matches.

• Searches will be limited to specific records and, unless otherwise noted, will be one-time searches.

• If a financial institution identifies a match for a named subject, the institution need only respond to FinCEN that it has a match and provide point-of-contact information for the requesting law enforcement agency to follow up directly with the institution.

On the whole, these provisions are the most effective means of detecting terrorist financing because the industry is simply looking for names of individuals being investigated by the government for terrorist activity. For example, according to FinCEN, between April 1, 2003, and April 26, 2004, the Internal Revenue Service submitted 16 requests to FinCEN pertaining to 66 individuals and 17 businesses. These requests generated 646 positive matches with more than 1,274 financial institutions. Since Section 314(a)'s creation, the system has been used to send the names of 1,547 persons suspected of terrorism financing or money laundering to more than 26,000 financial institutions and has produced 10,560 matches that were passed on to law enforcement.

Other Options

As we grapple with how to prevent terrorist financing from entering the legitimate financial system, what is available beyond the section 314 process? Clearly, the new obligations under the USA PATRIOT Act do not directly address the nature of how monies enter a system to support terrorism. The various sources for banks are the FATF "typologies" on terrorist financing and similar examples provided by U.S. law enforcement agencies such as FinCEN. What do they tell us? For example, a focus on charitable organizations or "non-profit organizations" (NPOs) is a constant theme.

According to FATF:

> Most countries share the concern over the difficulties in detecting terrorist financing through misuse of NPOs. It is generally acknowledged that such organizations play a crucial social and financial support role in all societies, and obviously this role is not called into question. Nevertheless, the sheer volume of funds and other assets held by the NPO sector means that the diversion of even a very small percentage of these funds to support terrorism would constitute a grave problem. Therefore, the limited knowledge about the extent to which terrorists may be exploiting the sector should be considered a matter of serious concern for the international community.

All this emphasizes that we are in a different world now, and the tracing or monitoring of monies for terrorist activities is not a simple task.

Conclusion

Much has been written about the PATRIOT Act and the necessity of quickly enacting laws to address terrorism. Debate still rages on whether the legislative response was appropriate to the attacks. On a positive note, it should be emphasized that the ABA supported the PATRIOT Act because it accomplished what other proposals in previous times could not — requiring non-bank institutions to have AML programs and procedures. To stem the financing of terrorism, however, government must commit to providing up-to-date intelligence to the financial sector. We have seen the beginning of that process, but it must be increased. Any other strategy is doomed to fail. ■

The opinions expressed in this article do not necessarily reflect the views or policies of the U.S. government.