Chapter 4

Combating Terrorist Financing in the United States: The Role of Financial Institutions

Since the 9/11 terrorist attacks, U.S. financial institutions have, almost uniformly, wanted to do everything in their power to prevent their use by terrorist operatives and fund-raisers. Indeed, law enforcement and intelligence officials have praised the private financial services sector for its willingness to assist in terrorist-related investigations. The effort is clearly there, but what about the results?

The current regulatory regime was designed primarily for discovering and reporting money laundering—the efforts of criminals, such as drug traffickers, to filter huge amounts of cash through the financial system. Only banks have the information needed to discover and report those kinds of transactions. A regulatory regime in which valuable data are passed from the banks to the government, in that context, makes sense.

For terrorist financial transactions, the amount of money is often small or consistent with the customer's profile (such as a charity raising money for humanitarian aid) and the transactions seemingly innocuous. As a consequence, banks generally are unable to separate suspicious from legitimate transactions. The government, however, may have information that would enable banks to stop or track suspicious transactions. As a result, financial institutions can be most useful in the fight against terrorist financing by collecting accurate information about their customers and providing this information—pursuant to legal process—to aid in terrorism investigations. At the same time, the government should strive to provide as much unclassified information to financial institutions as possible.

Terrorist Financing in the United States

The term "terrorist financing" is commonly used to describe two distinct types of activity. First, it can consist of the financing of operational terrorist cells, like the 19 hijackers who conducted the 9/11 attacks. This financing consists of the funds the cell needs to live and to plan, train for, and commit the terrorist act. The second type of terrorist financing is fund-raising—the process by which an organized terrorist group, such as al Qaeda or Hamas, raises money to fund its activities. Such fund-raising often takes place through nongovernmental organizations, which may raise money for legitimate humanitarian purposes and divert a fraction of their total funds for illicit purposes.

The funding of terrorist operations involves relatively small dollar amounts, from the estimated $10,000 cost of the 1998 U.S. embassy bombings in East Africa, to the estimated $400,000–500,000 for the 9/11 attacks themselves (of which roughly $300,000 passed through U.S. bank accounts over a period of nearly two years). The 9/11 attack provides a good case study of how a large terrorist cell can be financed in the United States. The hijackers moved money into the United States in three ways. They received

wires totaling approximately $130,000 from overseas facilitators in the United Arab Emirates and Germany; they physically carried large amounts of cash and traveler's checks with them; and some of them set up accounts overseas, which they accessed in the United States with credit or ATM cards. Once here, the hijackers opened bank accounts in their real names at U.S. banks, which they used just as millions of other people do to conduct the routine transactions necessary to their plan. The hijackers used branches of both large national banks and smaller regional banks.[46]

Nothing the hijackers did would have alerted any bank personnel to their being criminals, let alone terrorists bent on mass murder. Their transactions were routine and caused no alarm. Their wire transfers, in amounts from $5,000 to $70,000, were utterly anonymous in the billions of dollars moving through the international financial system on a daily basis. Their bank transactions, typically large deposits followed by many small ATM or credit card withdrawals, were entirely normal, especially for foreign students living in the United States. No financial institution filed a suspicious activity report (SAR) and, even with benefit of hindsight, none of them should have.[47] Contrary to numerous published reports, there is no evidence the hijackers ever used false Social Security numbers to open any bank accounts. In some cases, bank employees completed the Social Security number fields on the new account application with a hijacker's date of birth or visa control number, but did soon their own to complete the form.[48]

The use of a financial institution for a fund-raising operation looks entirely different from the use of an institution by a terrorist cell, like the 9/11 plotters. The transactions are often much larger. For example, the Benevolence International Foundation (BIF), an Illinois charity designated a terrorist supporter by the U.S. government in 2002, received more than $15 million in donations between 1995 and 2000.[49] Funds are likely pooled from multiple small donors and then sent overseas, frequently to troubled places in the world under the auspices of a charity. For example, the Global Relief Foundation (GRF), another Illinois charity designated a terrorist supporter by the U.S. government in 2002, annually sent millions of dollars overseas, especially to such strife-torn regions as Bosnia, Kashmir, Afghanistan, Lebanon, and Chechnya. According to its IRS filings, GRF sent $3.2 million overseas in 1999 and $3.7 million in 2000. Like the financing of a cell such as the 9/11 hijackers, however, a competent terrorist fund-raising operation will not be apparent to bank personnel. The money sent overseas will not go to al Qaeda or any designated terrorist group. Instead, the money will go to an overseas office of the charity or an affiliated charity, and the diversions to terrorist facilitators or operatives will likely

[46] See appendix A (discussing 9/11 transactions in detail).
[47] As discussed later, U.S. law requires banks to report potentially criminal financial activity by filing SARs with the Financial Crimes Enforcement Network (FinCEN) within 30 days of the suspicious transaction.
[48] This is not to say that the hijackers were experts in the use of the U.S. financial system. For example, the teller who opened an account for plot leaders Atta and al Shehhi spent an hour with them, explaining the procedures for ATM transactions and wire transfers, and one branch refused to cash a check for al Shehhi on one occasion because he presented IDs with different addresses. This incident led the bank to issue a routine, internal security alert to watch the account for possible fraud, but provided no basis for concern about serious criminality—let alone terrorism. These minor blips provided no clue to the financial institution about the hijackers' murderous purpose.
[49] Whether BIF actually funded al Qaeda remains an open question. See chapter 6.

take place overseas. In the current environment, the donors presumably will not include pro-Jihad comments on the memo line of their checks, as did pre-9/11 donors to one suspect charity the FBI investigated. The fund-raising operation will look to the bank like a charity sending money to troubled parts of the world—which it is doing, at least in part.

Why Suspicious Activity Reporting Works for Money Laundering But Is Less Useful for Terrorist Financing

The Bank Secrecy Act (BSA) regime, described below, was designed to combat money laundering and related offenses and, assuming that it is well-implemented and well-enforced, it is reasonably effective for this purpose. However, the requirement that financial institutions file SARs does not work very well to detect or prevent terrorist financing, for there is a fundamental distinction between money laundering and terrorist financing. Financial institutions have the information and expertise to detect the one but not the other.

The Bank Secrecy Act—what it is and what it does

The premise behind the money-laundering laws and regulations was that because the underlying crimes generate enormous amounts of cash, criminal enterprises need to convert that cash into something less traceable and more usable. In perhaps the best-known example of money laundering, Russian and U.S. shell corporations were able to move billions of dollars through correspondent accounts owned by foreign banks at the Bank of New York and Citibank. Likewise, Raul Salinas, the former president of Mexico, was found to have laundered millions of dollars in alleged public corruption money through Citibank accounts. The role of Mexican banks was highlighted in a U.S. law enforcement investigation known as Operation Casablanca, which found that millions of drug-tainted dollars had been laundered through Mexican banks.

The United States' method to prevent criminals from taking advantage of the financial system relies on the basic premise that financial institutions—not the government—are in the best position to detect money laundering and related illicit transactions. Thus, the law imposes on financial institutions the obligation to report suspicious activity that involves their use. This law and related regulations, generically referred to as the "Bank Secrecy Act," require banks (and now a host of other financial institutions, including broker-dealers, credit card companies, insurance companies, and money service businesses)[50] to understand, control, and report transactions that may have a questionable origin or purpose. Specifically, banks are required to report cash transactions in excess of $10,000, as well as any other transactions they deem "suspicious."[51]

[50] For purposes of this discussion, we use the term *bank*, although in most respects the obligations extend to other financial institutions.

[51] Additionally, banks must ensure that they do not unwittingly engage in transactions with individuals listed on Treasury's list of prohibited persons, maintained by the Office of Foreign Assets Control (OFAC). Such transactions are prohibited by a number of statutes tied to the president's ability to bar U.S. persons

The SAR requirement is at the core of the government's anti-money-laundering effort. Inherent in a bank's responsibility to report (or refuse to conduct) a suspicious transaction is an obligation to have sufficient knowledge of its own transactions and customers to understand what is suspicious. This requires a bank to "know" its customer—who the beneficial owner of an account is, what the customer's likely transactions should be, and what, in general, is the source of the customer's money. Once it understands its customer and the customer's likely transactions, the bank is able to determine whether the customer is conducting transactions out of character for that profile. Additionally, understanding the customer's probable transactions enables the bank to assess the risk that the account will be used to launder money, and will in some respects determine how closely the institution monitors the customer's account. A bank's failure to report suspicious activities, or to have a system in place that could reasonably detect suspicious financial transactions, is punishable by some combination of administrative sanctions, civil fines, and criminal penalties.

A bank can best detect suspicious transactions at one of two points. The "front end" of a transaction involves the tellers and other individuals who may have face-to-face contact with the customer and can often determine if a specific transaction is worth a second look. A bank will typically train tellers and other such individuals to look for specific "red flags" to determine if a transaction is suspicious. The second likely point of detection occurs in the "back office"—an analysis of financial transactions, which takes place in a specialized unit, for example, or in particularly high-risk areas such as the bank's wire transfer operations. Money-laundering analysts look at the bank's transactions to determine if they can conclude, by examining patterns of transactions, whether those patterns are suspicious.

Analysts are aided significantly by software that is programmed to catch "anomalies" (i.e., unusual financial transactions) that are indicative of money laundering. The key is to find those transactions that would be out of character for the customer's purported business activity. A large cash deposit would not be suspicious for a customer like Wal-Mart, but it would be for a customer whose only reported source of income is a Social Security check. Sophisticated software should be able to distinguish between such transactions and alert the money-laundering compliance analyst at the bank to investigate further. This software, however, is not self-executing. It must be set up and fine-tuned. Such adjustments can only be done by the bank itself; they require a deep and thorough understanding both of the bank's ordinary business and of its potential high-risk product lines and high-risk customers. Additionally, the bank typically has specialists with a fairly sophisticated understanding of money laundering. Because money laundering must involve large transactions, banks are able to safely ignore a significant percentage of their transactions that fall below specific thresholds.

---

from trading with an enemy of the state. Violations of these prohibitions are enforced by criminal penalties or by civil fines, depending on the seriousness of the offense, among other factors. The listing process, described elsewhere, is generally considered to be too cumbersome to be of use in detecting operational elements of terrorist organizations.

If further review does not dispel suspicions, the bank is required to file a SAR within 30 days from the discovery of the suspicious conduct. (When a bank cannot identify a suspect, it has an additional 30 days to try to do so.) The bank must also monitor the account and should refuse to engage in future transactions it deems to be suspicious. In some cases, it may terminate the relationship with the customer.

The BSA regime also reflects sensitivities concerning financial privacy. A system requiring bank reporting was thought to be less intrusive than allowing unfettered government surveillance of bank records. The specter of a bank "knowing its customer" is somewhat less threatening than the idea that the government ought to understand and know all of a citizen's probable financial transactions.

As a result of the BSA regime, most money launderers, drug dealers, and high-level fraudsters understand that trying to pump massive amounts of cash through a U.S. bank is fraught with peril. As a result, they generally prefer instead to use other, less risky, methods to move money—sending it in bulk across our porous borders, for example, or through a less-regulated industry like money-transmitting services. If they do use banks, they take care to structure smaller transactions among dozens of different accounts—less risky, to be sure, but considerably slower and more costly.

The terrorist-financing model

The model of banks having superior knowledge to detect illicit activity may not apply to terrorist financing. Although the U.S. government may possess the intelligence that could reveal terrorist operatives and fund-raisers, financial institutions generally do not. The 9/11 operation provides a perfect example. The 19 hijackers hid in plain sight: none of their transactions could have revealed their murderous purpose, no matter how hard the banks looked at them (see appendix A). Intelligence the government had, however, could have been critical to identify the terrorists among us. For example, the U.S. government had reason to believe that future hijackers Khalid al Mihdhar and Nawaf al Hazmi were al Qaeda operatives in the United States. Both these terrorists had U.S. bank accounts, but bank personnel never could have suspected that their customers were terrorists no matter how diligently they studied the transactions, which were utterly routine.

Since September 11, financial institutions and the government have made efforts to create a financial profile of terrorist operatives. The FBI examined the financial transactions of the 9/11 hijackers and came up with some distinguishing features: they arrived at banks in groups; they listed their occupation as students; they spent a large percentage of their income on flight schools and airfare, particularly first-class airfare; and they were funded in large part through wire transfers from the UAE. This profile might help detect another plot exactly like 9/11, but we can expect that the next plot will look entirely different. As a result, this profile does not especially help banks find future terrorist operatives, who we can expect will make different, although equally routine, use of the financial system. In fact, no effective financial profile for operational terrorists located in the United States exists. The New York Clearinghouse, a private consortium of the largest money-center banks, attempted to put together such a profile in partnership with government investigators. After two years, they concluded it could not be done.

Creating a profile for terrorist fund-raising groups is not necessarily any easier. An Islamic organization that collects funds from small donors, pools the funds, and then sends large monthly wire transfers to Chechnya, Afghanistan, Kashmir, or the West Bank could be a jihadist or terrorist fund-raising operation, or an entirely legitimate humanitarian operation devoted to serving civilians in impoverished and war-torn regions of the world. The government may have information (derived from sources such as electronic surveillance or human intelligence) from which it can distinguish between the two rationales for the transactions, but it is unlikely that banks will be able to tell the difference from the transactions themselves.

The government has also tried to describe suspicious activity indicative of terrorist fund-raising. The Financial Crimes Enforcement Network (FinCEN) conducted a comprehensive analysis of potential terrorist-financing patterns, which it published in January 2002. Drawing on actual SARs filed by banks, it described five cases that might have been examples of terrorist fund-raising. Ultimately, these cases centered on financial transactions indicative of money laundering that involved, as FinCEN delicately put it, "nationals of countries associated with terrorist activity."[52] This analysis appears to be of little use in ferreting out a sophisticated terrorist fund-raising operation, which will likely look to the bank identical to a legitimate Islamic charity.

Although FinCEN took great pains to caution that country of origin or ethnicity should not, absent other factors, be taken to indicate potential criminal activity, the report highlights a problem with applying the BSA regime to terrorist financing. The inability to develop meaningful indicia of a terrorist cell or terrorist fund-raising operation creates a risk that financial institutions could rely primarily on religious, geographic, or ethnic profiling in an attempt to find some criteria helpful for identifying terrorist financing. Such profiling raises a number of problems. Fundamentally, it will not be an effective means to combat terrorist financing. The vast majority of Islamic or Arab bank customers are not terrorists or terrorist supporters, so indiscriminately filing SARs on them will do nothing but waste resources and cause bad will. Similarly, reporting that an Islamic charity is sending money to Afghanistan will not be particularly effective in finding terrorist financiers; there are certainly many legitimate humanitarian needs there. In addition to doing little good, this type of profiling may subject customers to heightened scrutiny without legitimate basis, and could even extend to refusing to service customers meeting a certain profile. Of course, religion, nation of origin, or ethnicity can and should be taken into consideration, along with many other factors, in the subjective judgment as to whether a certain transaction or account is suspicious. Our point is that profiling—by itself—is both an unfair and an ineffective way for financial institutions to attack terrorist financing.

[52] FinCEN, *SAR Bulletin*, no. 4 (Jan. 2002). Typically, they included structuring multiple deposits or other transactions to be below the $10,000 reporting threshold, collecting funds through a variety of financial channels then funneling them to a small number of foreign beneficiaries, or a volume of financial activity inconsistent with the stated purpose of the account.

That being said, there may be utility in having financial institutions examine transactions for indicia of terrorist financing. It certainly assists in preventing open and notorious fund-raising and forces terrorists and their sympathizers to raise and move money clandestinely, thereby raising the costs and risks involved. The deterrent value in such activity is significant and, while it cannot be measured in any meaningful way, ought not to be discounted.

Financial Institutions Have a Role in Combating Terrorist Financing in the United States

The inability of financial institutions to detect terrorist operatives or terrorist fund-raising does not relegate the private sector to the sidelines in the fight against terrorism. To the contrary, there are a number of things that financial institutions can do right now. There also are a number of things that could be done in the future, if current law or government policies are changed. This section addresses what can be done now and assesses some possibilities for the future**.**

Now: Helping the government find the terrorists

Financial tracking

Although financial institutions lack information that can enable them to identify terrorists, they have information that can be absolutely vital in finding terrorists. If the government can determine where a terrorist suspect banks, his account opening documents can provide his address, and his ATM and credit card usage can show where he is and what he is doing. Again, the 9/11 plot provides a good example. Had the U.S. government been able in August 2001 to learn that hijackers Nawaf al Hazmi and Khalid al Mihdhar had accounts in their names at small New Jersey banks, it could have found them. The hijackers actively used these accounts, through ATM, debit card, and cash transactions, until September 10. Among other things, they used the debit cards to pay for hotel rooms—activity that would have enabled the FBI to locate them, had the FBI been able to get the transaction records fast enough. Moreover, al Hazmi used his debit card on August 27 to buy tickets on Flight 77 for himself, his brother, and fellow Flight 77 hijacker Salem al Hazmi.

If the FBI had found either al Mihdhar or Nawaf al Hazmi, it could have found the other. They not only shared a common bank but frequently were together when conducting transactions. After locating al Mihdhar and al Hazmi, the FBI could have potentially linked them through financial records to the other Flight 77 hijackers. For example, as noted, Nawaf al Hazmi used his debit card on August 27 to buy plane tickets for himself and his brother, linking those two hijackers. Nawaf al Hazmi and Flight 77 pilot Hani Hanjour had opened separate savings accounts at the same small New Jersey bank at the same time and both gave the same address. On July 9, 2001, the other Flight 77 muscle hijacker, Majed Moqed, opened an account at another small New Jersey bank at the same

time as Nawaf al Hazmi, and used the same address. Given timely access to the relevant records and sufficient time to conduct a follow-up investigation, the FBI could have shown that Hani Hanjour, Majed Moqed, and Salem al Hazmi were connected to potential terrorist operatives al Mihdhar and Nawaf al Hazmi. No one can say where the investigation would have gone from there, but financial records could potentially have been used, along with other information—including perhaps information found in the possession of or provided by the Flight 77 hijackers—to link the Flight 77 hijackers to the others and, perhaps, disrupt the plot.

Unfortunately, this theoretical investigation would not have worked quite as smoothly in the world that existed before September 11. First, an agent attempting to locate the hijackers would have needed to know where to look. There are thousands of financial institutions in the United States, and making an inquiry of each one of them, regardless of the exigency of the situation, would not have been a realistic enterprise. Even an experienced agent tasked to find al Mihdhar or al Hazmi would have been unlikely to think to use financial tracking; and an agent who did probably would have first called those institutions with which he or she had some personal relationship—probably big banks.

Moreover, before 9/11 financial investigations almost always moved at a slow, methodical pace. In a typical investigation, a financial institution received a grand jury subpoena or a National Security Letter (NSL) from a federal prosecutor or agent. The subpoena had a return date—the date by which the bank was required to produce the records requested. In a typical investigation, the bank searched its records and produced hard copies of the material requested. Banks and other financial institutions then needed substantial time to locate and produce records, even in response to a lawful subpoena. Financial institutions had been prohibited from giving law enforcement certain records absent compulsory legal process.

Before 9/11, the U.S government did not think in terms of financial tracking, certainly not systematically and on an urgent basis. The terrorist attacks changed this thinking. Since 9/11, the government uses financial information to search out terrorist networks so that a known suspect like al Mihdhar could be quickly located. There are now two primary approaches for doing this: FBI outreach that has enhanced private sector cooperation and Section 314(a) of the USA PATRIOT Act.

The FBI's Terrorist Financing Operations Section (TFOS) has taken the existing legal rules, which were developed within the context of traditional after-the-fact investigation of financial crimes, and created a systematic approach to gain expedited access to financial data in emergencies. To facilitate emerging situations, the FBI has compiled a list of high-level contacts within the financial community—banks, brokerage houses, credit card vendors, and money services businesses—to whom it can turn to get financial information on an expedited basis at any time, including nights, weekends, and holidays. The FBI serves them on an expedited basis with a subpoena or other legal process to get the relevant data. In true emergencies, the FBI can get information quickly to locate an individual or find links among co-conspirators.

Applying the post-9/11 FBI approach to the pre-9/11 search for al Mihdhar and al Hazmi strongly suggests the current system would have enabled the hijackers to be quickly located. Indeed, the recently retired founder and chief of TFOS stated that given the same circumstances today, the FBI would find al Mihdhar "in a heartbeat."[53] Corroborating this contention, FBI has successfully used its system a number of times to locate terrorist suspects and prevent terrorist attacks. For example, after the FBI received information that certain potential terrorists had infiltrated the United States, TFOS put into practice the process it had developed to track the suspects through their financial transactions. The TFOS process proved successful in obtaining useful data in a very compressed time frame. Although the subjects proved not to be terrorists, the system demonstrated its capability. The FBI's ability to do near real-time financial tracking has enabled it to locate terrorist operatives in a foreign country and prevent terrorist attacks there on several occasions. The system also helped crack a major criminal case, played a role in clearing certain persons wrongly accused of terrorism, and has proved very valuable in vetting potential threats.

The second approach to obtaining basic financial information on an expedited basis is through a regulation issued under Section 314(a) of the USA PATRIOT Act. By this regulation, the Department of Treasury requires financial institutions upon the government's request to search their records and determine if they have any information involving specific individuals. Financial institutions must report any positive matches to law enforcement within two weeks after the request for information. If there are matches, law enforcement must follow up with a subpoena to obtain the actual transaction records as discussed above. In an emergency, law enforcement can ask Treasury to require banks to respond more quickly to the request, sometimes in two days, a procedure that they have used on several occasions thus far.

In practice, this process enables law enforcement to find out if an individual of interest has accounts or has conducted transactions in any one of thousands of financial institutions across the country. It saves an investigator hundreds of hours that would have otherwise been spent on a bank-by-bank inquiry—an inquiry that would not have been done under the old system owing to time and resource constraints. One agent told the Commission staff that the new procedure so far has produced "tremendous results." She cited an instance in which a terrorism investigation resulted in the discovery of two bank accounts using conventional investigative techniques. Then, as a result of the Section 314 process, investigators were able to identify 19 other accounts across the country—accounts that they would have never been able to find otherwise.[54]

---

[53] By contrast, he said that while it would have been theoretically possible to use financial tracking to find the hijackers before 9/11, the probability of doing so in a timely fashion would have been extremely low.

[54] One concern about the Section 314 process is the possibility that a request to thousands of financial institutions will cause the information to be leaked. In a Las Vegas criminal investigation in October 2002 and a New York terrorism case in March 2003, the media published the fact of the law enforcement requests. In the New York case, the *New York Post* even called the subjects to ask them why the FBI was making the request. As a result, the FBI conducts a risk-benefit analysis before making each request. There are civil and criminal penalties in the event of a disclosure, and Treasury includes a warning with every request. There is no guarantee, however, that such warnings will be sufficient to deter leaks.

Account opening and customer identification procedures/data retention

Financial institutions play a critical role in any effort to find terrorists under either the FBI's system or Section 314. To fulfill this role properly in the life-and-death emergencies that can arise, financial institutions must (1) know their customers by their real names and possess other essential identifying information, (2) have the ability to access this information in a timely fashion, and (3) quickly provide this information to the government in a format in which it can be effectively used.

Section 326 of the USA PATRIOT Act requires that financial institutions "enhance the financial footprint" of their customers by ensuring effective measures for verifying their identity. Section 326 recognized that effective customer identification may deter the use of financial institutions by terrorist financiers and money launderers and also assist in leaving an audit trail that law enforcement can use to identify and track terrorist suspects when they conduct financial transactions. In May 2003 the Department of the Treasury issued regulations implementing the statute, setting forth the type of information that must be collected as well as the acceptable methods for verifying identity.

The need for accurate identifying information puts a premium on financial institutions having effective account opening procedures that vet the true identify of each customer, to the extent possible. A name search for Khalid al Mihdhar will not find him if he is banking under another name. Obviously, banks cannot be expected to detect perfectly forged passports and other identification documents; but terrorists rarely are perfect, and training in spotting false identification documents could help bank personnel catch the most egregious examples. In addition, bank personnel must ensure that account documents reflect the full and accurate name of the customer, even if that name is long.[55] Equally important, banks must obtain and accurately record key identifying information about their customers, including date of birth, Social Security number, and passport number. Many names are so common that nationwide searches for them would generate so many false positives as to be useless in an emergency. At times, however, the FBI can obtain and provide other identifying information, such as a passport number, which can be crucial in narrowing the search—provided that the institution where the subject is a customer has that information.

The need to locate terrorist operatives in the most exigent circumstances means that financial institutions must be able to access their data quickly. Quick retrieval can be a problem for some financial institutions, where years of piecemeal information-system upgrades have created a dysfunctional structure that greatly complicates the task of determining if a particular person is a customer. For example, an official of one midsize

[55] Shortening the name could mean that the account will be missed if the FBI is seeking a permutation different than the one used. For example, Ali Abdul Aziz Ali, a.k.a. Ammar al Baluchi, a key facilitator of the 9/11 attacks, would not be found if a bank listed him only as Abdul Aziz Ali and the FBI was looking for Ammar al Baluchi.

regional bank told Commission staff that his institution must email 28 different people to respond to a Section 314(a) request. Some banks simply lack electronic searching capability altogether. An FBI agent with a leading role in the Bureau's financial-tracking effort said that many financial institutions can search their data only manually, which is both resource-intensive and painfully slow in an emergency. Ideally, financial institutions should be able to do quick electronic searches by customer name, by other identifying information such as Social Security number or date of birth, or even by address or employment. Many financial institutions lack this ability today.

Once a financial institution has informed the government that a suspect is a customer and has received appropriate legal process, it can assist law enforcement greatly by providing continuous updates about the suspect's transactions. For example, the information that the suspect just used his credit card to rent a hotel room, book an airline flight, or rent a Ryder truck can be essential in an emergency. Many sophisticated financial institutions can provide the FBI with near "real-time" information on a suspect's activities, but other institutions entirely lack this capability, owing to technical limitations.

Finally, upon receipt of legal process, financial institutions must be able to communicate the relevant account information to the government officials quickly and efficiently. For many types of information, this means in electronic format. Although the FBI has long lagged behind the rest of the country in information systems technology, it has made tremendous strides since 9/11 in using available technology to find terrorists suspects, especially through TFOS's financial-tracking efforts. In many cases, emergency tracking can be streamlined if information is provided to TFOS in electronic format. Many financial institutions lack this capability, however.

The FBI's ability to find terrorist suspects in an emergency through financial tracking depends in large part on the private sector's voluntary cooperation. By all reports, the financial sector's cooperation has been immense since 9/11, but there is a risk that cooperation will decrease as the terrorist attacks fade into history and antiterrorism efforts become just another cost center for financial institutions. Government misuse of emergency procedures in non-emergency situations could also substantially reduce the likelihood that the private sector will respond when its help is truly needed to save lives. To avoid this problem, it is critical that law enforcement and the financial community maintain good lines of communication. This communication is important at all levels. Industry groups and major national institutions must meet regularly with national law enforcement leaders, such as the senior agents running FBI TFOS and the director of FinCEN, to focus on larger strategic issues. At the same time, FBI field offices need to reach out to smaller regional financial institutions, which they may need to contact in an emergency.

This is not to say that financial institutions should become simply another appendage of law enforcement. To the contrary, under either the FBI approach or Section 314(a), without legal process financial institutions can answer only one basic question: does X have an account at your bank? Everything beyond this question requires legal process under current law. It is hard to see why any privacy or liberty concerns should be raised

about the private sector and financial institutions working together to develop streamlined procedures for providing critical data quickly in an emergency—pursuant to a lawful subpoena or other process.

The future: What more can be done?

A number of proposals have been made in recognition that the traditional BSA approach is inadequate to address the challenges of terrorist financing.

Sharing classified information with bank personnel: A bad idea

The BSA model fails with respect to terrorist financing because the government—not the financial institutions—has the information that can best identify the terrorist operatives or fund-raisers. Some have proposed correcting that problem by providing security clearances to financial institution personnel and then providing these cleared officials with classified intelligence about terrorist financing. The idea is that the cleared bank personnel, armed with intelligence to give them a better idea of what they are looking for, will be able to ferret out the terrorists among their customers.[56]

The idea of clearing financial institution personnel may be attractive on its face, particularly to those unfamiliar with the nature of financial intelligence. The proposal would likely do little, however, to help banks combat terrorist financing and creates a number of serious privacy and civil liberty concerns. Most intelligence on terrorist financing is not actionable—it does not identify specific terrorist financiers and their accounts with sufficient precision to allow actions to disrupt the activity. The intelligence tends to be limited and speculative, and it frequently relies on dubious sources of information. It can be valuable to trained intelligence experts, who can evaluate it in the context of the broad spectrum of available information, but not to bank compliance directors, who will necessarily lack the time and current knowledge to properly evaluate it. Even if bank personnel have time and expertise, the intelligence rarely will yield information that they would find useful, such as names of specific account holders.

To the extent that the intelligence community can generate specific names or accounts, such information can usually be shared with banks in an unclassified way. Banks can be told to be aware of person X from country Y without needing to know how that information was obtained. If the intelligence community develops patterns or trends, this information presumably also can be shared with financial institutions without need for security clearances.

[56] See, e.g., testimony of former National Security Council official Richard A. Clarke, Senate Banking, Housing and Urban Development Committee (October 22, 2003) (clearing bank compliance personnel will "bring us back great benefits because then they'll know what to look for"). Representatives of financial institutions made similar recommendations to Commission staff.

Providing intelligence about terrorist financing to bank personnel raises serious privacy and civil liberty issues. People may be named in intelligence reports, but many of the allegations within these reports are unproven. Some reports prove to be entirely baseless. Turning these reports over to private citizens like bank personnel runs the risk that entirely unsubstantiated allegations may lead banks to shut customer accounts or take other adverse action. Even assuming that the classified information itself is never leaked, the names of people identified in the intelligence cannot be kept secret. When the bank compliance officer who receives the secret intelligence asks for scrutiny of a customer's accounts for no apparent reason, other bank personnel will likely surmise that classified information drove this request.

Supporters of giving security clearances to bank personnel point out that the U.S. government regularly clears private citizens, such as employees of defense contractors. There are, however, few if any instances in which the U.S. government provides classified information potentially adverse to U.S. citizens to private actors for the specific purpose of causing those private actors to subject the U.S. citizens to greater scrutiny.[57] Creating such an unusual and potentially dangerous situation cannot be justified by the minimal benefits that sharing classified information might produce.

Broad government access to private data: Perhaps someday

A more radical, but perhaps far more effective, proposal would give government authorities direct unfettered access to private financial data for the limited purpose of finding or detecting terrorist operatives or fund-raisers.[58] Under this approach, counterterrorist officials would be able to access privately held data by using computer technology to search for known terrorist suspects by name, data of birth, Social Security number, or other identifying information, which would find terrorist suspects living under their own name and also help identify others living under assumed names. The government could also use privately held financial data in conjunction with a wide variety of other data to link a suspect to his or her associates. As one former government official testified to the Commission: "Counterterrorism officers should be able to identify known associates of the terrorist suspect within 30 seconds, using shared addresses, records of phone calls to and from the suspect's phone, emails to and from the suspect's accounts, financial transactions, travel history and reservations, and common memberships in organizations, including (with appropriate safeguards) religious and expressive organizations."[59] The government is currently far from these capabilities, and

[57] The commonality of many names, especially Arabic names, compounds the potential for mayhem. For example, an official of one major financial institution told Commission staff that there were 85 Mohamed Attas in New York City alone. Intelligence reports of varying quality may provide the basis for bank action against not only the persons alleged to be involved in terrorist financing but innumerable people with the same or similar names.

[58] See, e.g, *Creating a Trusted Network for Homeland Security*, Second Report of the Markle Foundation Task Force (Dec. 2003), appendix F ("Within 30 seconds [of learning the identify of a terrorist suspect], the counterterrorism agency should be able to access U.S. and international financial records associated with the suspect").

[59] Prepared testimony of Stewart Baker, Dec. 8, 2003.

significant technical, legal and privacy hurdles would need to be crossed before it would have anything remotely approaching this ability.

Supporters of this approach contend that privacy would be protected through anonymity and technology. The data of millions of people could be electronically searched but all individuals would remain anonymous except those identified as terrorist suspects, who would then be subjected to further scrutiny. Sophisticated technology would control access to the data, electronically audit the data and keep a detailed record of exactly who accessed it for what purpose, and ensure the anonymity of persons whose data are searched.

If such a system existed, it would be tremendously useful in looking for known terrorist operatives living under their own name, such as al Mihdhar or al Hazmi, or future hijackers living under false identities. Technology could be imagined that would scan masses of financial data looking for terrorist fund-raising operations as well, while preserving the anonymity of the data belonging to persons whom it does not identify as potential terrorist fund-raisers.

Of course, major technological improvements would be required to implement this kind of a system. Currently, financial records are spread out across the country in thousands of financial institutions, each with its own data collection and retrieval system and level of technological sophistication.[60] There is no single database that the government can tap even in an emergency.

Even if such a database could be created, sweeping legal changes would be required to use it. The government does not have unfettered access to this financial information under current laws. Although the Supreme Court has stated that an account holder does not have an expectation of privacy in information he or she gives to another, such as a bank, there are a number of restrictions on the government's right to obtain such data. Most fundamentally, the government can obtain financial information or data only by lawful process, such as a grand jury subpoena or an NSL, for a particular case or investigation. The government has no general authority to access the entire country's financial records en masse, so that it can scan them to find potential terrorists or criminal suspects. Instead, an inquiry has to be made of each financial institution for each investigation.

Pushing the technological and legal limits even further is the idea that the government could develop the technology to sift through all the financial data that exists and create a program able to single out those financial transactions that are inherently suspicious.

---

[60] Banks and other financial institutions keep records as a part of the operation of their ongoing businesses. Financial institutions are generally required to keep financial information on hand, in a retrievable form, for five years. In contrast, other industries whose records would also be of use to counterterrorism investigators, such as Internet service providers, are not required to keep transaction records for any length of time and can (and do) regularly destroy them unless law enforcement requests that they be maintained. This has often been a source of frustration to law enforcement and intelligence agents, whose investigations are often hampered in the digital age by lack of a uniform and mandated record retention policy for internet service providers.

These ideas have been discussed in the open literature and have triggered major controversy and speculation. The Department of Defense's "Total Information Awareness" program, complete with its logo of an all-seeing eye, was a prime example of this type of technology. This research program sought to use sophisticated technologies to detect terrorist planning activities from the vast data in cyberspace; in other words, it sought to "pick the signal out of the noise." Congress has prohibited the funding of such a program, largely because of privacy concerns. Despite 9/11, it seems that privacy concerns will prevent anything remotely like these ideas from becoming reality in the foreseeable future.

That is not to say research should not go forward. Government and the private sector can, and should, continue to work on technology that could scan vast amounts of financial data to find known terrorist suspects, while protecting the privacy of the innocent persons whose data are searched. Perhaps sophisticated technology can be developed that would even be able to pick out unknown terrorist operatives or fund-raisers by their financial transactions—currently a near impossibility. Legitimate concerns about privacy should not retard research that might someday make us safer and, at the same time, actually not infringe on privacy rights. Ideally, the research efforts should draw on both the law enforcement and intelligence expertise of the government and the sophisticated technology and data management expertise of the private sector. Obviously, no such technology should ever be implemented on real data without public acceptance that the technological and legal safeguards in place will be sufficient to ensure privacy. The development of such technology and any public acceptance of it remain, at this point, pure speculation.