IMPROVING FINANCIAL OVERSIGHT: A PRIVATE SECTOR VIEW OF ANTI-MONEY LAUNDERING EFFORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

MAY 18, 2004

Printed for the use of the Committee on Financial Services

Serial No. 108–87

U.S. GOVERNMENT PRINTING OFFICE

95–012 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

MICHAEL G. OXLEY, Ohio, *Chairman*

JAMES A. LEACH, Iowa
DOUG BEREUTER, Nebraska
RICHARD H. BAKER, Louisiana
SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
ROBERT W. NEY, Ohio
SUE W. KELLY, New York, *Vice Chair*
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
JIM RYUN, Kansas
STEVEN C. LATOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, JR., North Carolina
DOUG OSE, California
JUDY BIGGERT, Illinois
MARK GREEN, Wisconsin
PATRICK J. TOOMEY, Pennsylvania
CHRISTOPHER SHAYS, Connecticut
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
GARY G. MILLER, California
MELISSA A. HART, Pennsylvania
SHELLEY MOORE CAPITO, West Virginia
PATRICK J. TIBERI, Ohio
MARK R. KENNEDY, Minnesota
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
KATHERINE HARRIS, Florida
RICK RENZI, Arizona

BARNEY FRANK, Massachusetts
PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELAZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
DARLENE HOOLEY, Oregon
JULIA CARSON, Indiana
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
BARBARA LEE, California
JAY INSLEE, Washington
DENNIS MOORE, Kansas
MICHAEL E. CAPUANO, Massachusetts
HAROLD E. FORD, JR., Tennessee
RUBÉN HINOJOSA, Texas
KEN LUCAS, Kentucky
JOSEPH CROWLEY, New York
WM. LACY CLAY, Missouri
STEVE ISRAEL, New York
MIKE ROSS, Arkansas
CAROLYN MCCARTHY, New York
JOE BACA, California
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
RAHM EMANUEL, Illinois
DAVID SCOTT, Georgia
ARTUR DAVIS, Alabama
CHRIS BELL, Texas

BERNARD SANDERS, Vermont

Robert U. Foster, III, *Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

SUE W. KELLY, New York, *Chair*

RON PAUL, Texas, *Vice Chairman*
STEVEN C. LATOURETTE, Ohio
MARK GREEN, Wisconsin
JOHN B. SHADEGG, Arizona
VITO FOSSELLA, New York
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
TIM MURPHY, Pennsylvania
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina

LUIS V. GUTIERREZ, Illinois
JAY INSLEE, Washington
DENNIS MOORE, Kansas
JOSEPH CROWLEY, New York
CAROLYN B. MALONEY, New York
JIM MATHESON, Utah
STEPHEN F. LYNCH, Massachusetts
ARTUR DAVIS, Alabama
CHRIS BELL, Texas

CONTENTS

WITNESSES

TUESDAY, MAY 18, 2004

APPENDIX

IMPROVING FINANCIAL OVERSIGHT: A PRIVATE SECTOR VIEW OF ANTI-MONEY LAUNDERING EFFORTS

Tuesday, May 18, 2004

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to call, at 10:07 a.m., in Room 2128, Rayburn House Office Building, Hon. Sue Kelly [chairwoman of the subcommittee] presiding.

Present: Representatives Kelly, Hensarling, Garrett, Gutierrez, Inslee, Moore, Maloney, and Matheson. Also present was Representative Royce.

Chairwoman KELLY. [Presiding.] This hearing of the Subcommittee on Oversight and Investigations will come to order.

An effective money laundering system relies on a collaborative effort from the public and private sectors. This effort has received additional scrutiny recently due to problems at Riggs Bank, an instance where the public-private collaboration stumbled badly in protecting the public's best interest. It is evident that the public and private sectors must continue to improve the way that suspicious activity is detected, reported and analyzed.

Today we examine ways to improve the oversight and utilization of transaction information by regulatory and law enforcement agencies so the failures at Riggs are the last of their kind in our country.

The current enforcement structure we have put in place to enforce our anti-money laundering laws disperses various levels of responsibility through a convoluted group of Treasury bureaus and independent agencies. It resembles somewhat a bowl of spaghetti. While these agencies have been focused on efforts to oversee the safety and soundness of our financial institutions for decades, they must embrace new responsibilities which acknowledge that money laundering is no longer a second-tier issue for financial regulators.

Of particular interest to this subcommittee are proposals to simplify the governmental structure so that regulation and compliance for these laws are better unified, perhaps even under the auspices of a single entity.

Given the vulnerabilities exposed by the Riggs case, I am inclined to believe that the current structure is a relic of a foregone era and that substantive organizational reforms are necessary. At a bare minimum, Congress should begin now an active and thor-

ough assessment of proposals aimed at strengthening our enforcement regime. This subcommittee intends to do just that in the coming weeks and months, and therefore I look forward to testimony from some of our witnesses as to how we might significantly improve the effectiveness of our system without creating yet another layer of bureaucracy.

Our financial regulators must place a strong emphasis on compliance through rigorous oversight, taking swift and forceful action for non-compliance when necessary. This oversight includes working with the private sector to develop accurate risk assessments that enable examiners to focus on specific institutions, because resources need to be concentrated appropriately.

The continued leadership of the administration and the Treasury Department is essential to improving financial oversight. Earlier this year, President Bush signaled his commitment to the war against terror by proposing a 14 percent increase in funding for the Financial Crimes Enforcement Network. FinCEN plays a key role in efforts to stop financial crimes by working with the financial community and supporting local, State and Federal law enforcement and intelligence agencies.

The administration has also announced the creation of the Office of Terrorism and Financial Intelligence—the acronym for that they are using is TFI, Terrorism and Financial Intelligence—within the Department of the Treasury to unify, under one structure, the functions of several offices. I applaud the administration for its efforts to streamline and centralize our anti-money laundering efforts. There must be greater communication between FinCEN, law enforcement, banking regulators and financial institutions, and I believe this office was an important step toward improving this coordination.

Now we must work to bring the next steps into focus. As evidenced by the failures of Riggs Bank and its regulator, the OCC, it is time to explore further reforms that improve the overall structure of our anti-money laundering efforts. It is unacceptable that a Washington, D.C.-based bank with the largest embassy banking clientele allowed tens of millions of dollars to pass unnoticed and unreported through accounts belonging to Saudi Arabian government officials. This activity continued even after a consent order was put in place last year. The mechanisms we put in place to detect and report suspicious activity failed, and they failed repeatedly. We no longer live in a world where such failures can be tolerated.

I thank the witnesses for appearing here today. You are on the front line of these efforts, and I look forward to hearing your views on how we can continue improving financial oversight.

I turn now to our ranking member, Mr. Gutierrez.

[The prepared statement of Hon. Sue W. Kelly can be found on page 32 in the appendix.]

Mr. GUTIERREZ. Good morning, Madam Chairman, and thank you very much for calling this hearing today. It is important, especially given recent events, that we closely examine our anti-money laundering efforts and whether they are sufficient. I welcome the witnesses here today and look forward to their testimony.

I understand that many financial institutions are truly committed to this effort, and I welcome their suggestions for improving compliance. However, I am concerned about the commitment of the relevant regulators to this effort, because criminals will always seek out the weakest link in the chain and will exploit any lapses in supervision.

After September 11, the passage of the PATRIOT Act, bank regulators were given more tools to combat terrorist financing, building on the foundation of existing anti-money laundering efforts. I am truly troubled by the Riggs situation. It represents not merely a failure of one institution's internal controls but a fundamental flaw in its regulation. It is my understanding that the flaws in Riggs' systems were long-standing and systematic, dating back well before the PATRIOT Act.

The consent order of last week is something that should have happened 2 years ago, if not earlier. I don't understand why the OCC was not more vigilant on this front and why it took them so long to take these actions. September 11 was a wake-up call for the industry and should have been for regulators as well. Our safety depends on banks and bank regulators to be on the forefront, on the front lines and prevent terrorists from using international financial systems to fund their activities.

I understand that the regulators take the risk-based approach to examining books under their purview, and I can't imagine why Riggs' book of embassy business would not have placed them in a category demanding extra scrutiny.

I am very concerned that the regulator has not made this responsibility a higher priority or that their resources may be spread too thin to fulfill their obligations. I have previously expressed concern about the OCC's attempt to broaden their portfolio into areas that Congress has not authorized without commensurately increasing their operational budget. In fact, the Financial Services Committee is on record in agreement with me on this point.

This recent incident with Riggs makes me even more concerned about the OCC's operations, and I really believe they should be testifying here today. Chairwoman Kelly, I know you share my concerns here, and I hope we can work together to get the OCC to testify before our subcommittee regarding this issue. I want to know if they have actively looked at every major bank that could have potential terrorist financing issues and what steps they have taken to aggressively control these issues.

One final point: The OCC issued its findings late last Thursday, and Friday a Maryland woman called her congressman and she was very concerned about her account at Riggs Bank. She was referred to the Banking Committee staff, and she said she wanted to talk to the regulators. My staff supplied the phone number for the OCC's Customer Assistance Group, but, unfortunately, they don't operate on Fridays. They only work 4 days a week. They only talk to consumers 4 days a week and then only from 9 o'clock to 4 o'clock.

So that woman had to wait from Thursday until Monday before she could possibly reach someone at the OCC. I think this agency is not concerned about consumers, and I have doubts about their commitment to anti-money laundering efforts.

Thank you, again, Chairman Kelly, for calling this hearing and for your leadership on this vital issue.

Chairwoman KELLY. Thank you, Mr. Gutierrez, and it is my intention, as you know, to continue discussing with the various agencies who have this responsibility what we can do to make sure there are no more failures of this type.

Mr. Royce?

Mr. ROYCE. Let me begin by thanking the Chair for calling this hearing today, and I am very grateful for your interest and leadership on this topic.

I think we are very fortunate to have with us this morning two of the countries foremost experts on terrorism, and I think it is unfortunate that both Mr. Aufhauser and Mr. Emerson have for so long been right on their predictions about our long fight against terrorism.

In both cases, they have warned us that what we are in for is a long struggle against a movement, not an organization but a movement, and it is a movement of a very extreme arm of the Wahabi Sect that is determined to ruin our way of life.

From the perspective of a member of this committee and of the International Relations Committee, I could not agree more with the assessments that they have made. We cannot win the war on terror unless the global community works to cut off the flow of funds that terrorists use and that terrorists receive. Certain terrorist acts do not require vast amounts of funding; however, the costs of indoctrination, the costs of recruitment and sustainability for their operations are quite high. If these rogue terror groups have no financial support, it is very difficult for them to continue to operate effectively.

In my view, the question we need to ask as members of the committee is how can the Financial Services Committee play a lead role in the fight on terror? We have the world's best safety and soundness financial regulators. As a part of their job, these regulators are also tasked to enforce the Bank Secrecy Act and certain provisions of the PATRIOT Act. This committee needs to emphasize the importance of that role to these regulatory agencies.

I think we may need to create a new structure and we may need statutory changes whereby each safety and soundness regulator would have a designated group that works hand in hand with the newly created Office of Terrorism and Financial Intelligence in the Treasury Department.

The Bank Secrecy Act and the PATRIOT Act give our examiners a number of tools to fight terror finance. This committee should lead Congress down the path of creating an environment where financial intelligence is gathered and then is shared and analyzed and used appropriately and effectively.

As Mr. Aufhauser argued in his testimony that he is going to present to us, "Much of the information that is submitted to the government under the Bank Secrecy Act is merely lodged like a book like a library shelf without a card catalog," in his words.

In the absence of an express and pointed request from law enforcement, he says, "the information remains unexploited. Surely we ought to have an artificial intelligence program that red flags patterns and concerns for investigation without specific targeted in-

quiry." He is absolutely correct. Not only do we need to utilize the PATRIOT Act, but we need to use it to data mine and to uncover terrorist activity.

And, again, I thank Chairwoman Kelly for her leadership on this subject, and I very much look forward to hearing the testimony of our witnesses this morning.

Chairwoman KELLY. Thank you very much, Mr. Royce.

Ms. Maloney?

Mrs. MALONEY. In the interest of time, I am just going to place my comments in the record and wait for the testimony. Thank you.

Chairwoman KELLY. Thank you.

Mr. Hensarling, you have no statement?

Mr. Matheson?

Mr. Moore?

Mr. Garrett? Oh, all right.

We now turn to our panel of witnesses. Thank you. It is a pleasure to welcome back to the committee Mr. David Aufhauser, the former general counsel of the Treasury Department who is currently with the law firm, Williams & Connolly. While at the Treasury Department, Mr. Aufhauser was the Chair of the U.S. Government Coordinating Committee on Terrorism Financing and a leader in implementing the USA PATRIOT Act. Through his work, he has helped shape our war against terror.

I am also very pleased to introduce Mr. John J. Byrne, the director of the Center for Regulatory Compliance for the American Bankers Association. Mr. Byrne has over 20 years of experience in regulatory and educational efforts on money laundering, asset forfeiture, computer security, privacy and other general electronic banking and compliance issues. He was the first private sector recipient of FinCEN's Director's Medal for Exceptional Service.

In addition, the subcommittee welcomes Mr. Joseph—let me make sure I am pronouncing it, Cachey? Cachey—representing Western Union. Mr. Cachey is responsible for administering compliance with the requirements of the Bank Secrecy Act. Regulations of the Office of Foreign Assets Control and related anti-money laundering and anti-terrorist financing laws in 196 countries in which the Western Union conducts its business.

Our next witness is James Richards, a senior anti-money laundering executive at Bank of America. Mr. Richards was formerly a supervisor of the Narcotics Forfeiture Group as the Massachusetts district attorney. He is also a Canadian barrister and later served as the BSA compliance and financial intelligence director with Fleet Financial.

Finally, the subcommittee will hear from Steven Emerson, the executive director of the Investigative Project, a well-known expert on international terrorism and terrorist financing. Mr. Emerson has shared his very important insights with this subcommittee on a number of occasions in recent years. His expertise is based on daily contact with sources in government and key financial institutions as well as his participation in major terrorist financing cases.

I thank all of our witnesses for your appearance here today and for your testimony. Without objection, your written statements will be made part of the record. You will each be recognized for a 5-minute summary of your testimony. I don't know if anyone needs

this, but I am going to remind you that there is a box on the end of each table. The green light means you have 5 minutes for your testimony, the yellow light means there is one minute remaining, and the red light means that we would like you to summarize your testimony. If you haven't gotten to the end, please summarize and let us move on to the next witness. Thank you very much.

And let us begin with you, Mr. Aufhauser. Thank you very much for being here.

STATEMENT OF DAVID D. AUFHAUSER, COUNSEL, WILLIAMS AND CONNOLLY LLP

Mr. AUFHAUSER. Thank you. It is an honor to be here. When I was at a Treasury I had a big staff and so I would get my testimony in early. I apologize that I got it into you about 7 minutes ago.

Chairwoman KELLY. Don't worry about that Mr. Aufhauser. It is valuable one way or another, so we accept it.

Mr. AUFHAUSER. For that reason, I am actually going to refer to much of it, but I think I can do it in 5 minutes. It was written knowing how this committee operates.

Probably one of the most vexing issues that this committee faces is the unprecedented nature of the threat of terrorism. The DNA of war has changed and changed inalterably. Confirming the asymmetry power of our military, no force is going to confront the United States on a conventional battlefield, at least currently, with a uniformed army under a recognized flag of state. Nor is there, importantly, a finite list of strategic targets to bunker with concrete and steel. Rather, the highest of profile targets are said to be soft, open to the most outrage and the most unspeakable scenes of mayhem. It is a school bus, it is a marketplace, it is a monument, it is a place of worship, indeed, it is this hall of Congress.

The greatest infamy, of course, in this uncommon war is the premium placed on the death of innocent people. Bullets and boots on the ground will not alone protect us. This is shadow warfare and it requires a rethink of how do you defend a nation. Every element of national power must be brought to bear, even the finance ministry of the United States, as anomalous as that may sound to folks.

With so many targets that defy military purpose and, therefore, escape common measures of detection, the three most critical factors that emerge as you talk about forging a new national power defense are, one, the need for enhanced intelligence, two, the leveraging effect of disrupting the logistical lines that constitute the purchase for stealth, and the need for a genuine partnership between business and government.

The funding of terror, the financing of terror, the money of terror is the one common denominator in all three theorems. First, as Congressman Royce pointed out, it is virtually the only intelligence that has true integrity in this war. The rest is a product of deceit or treachery or bribery or betrayal and sometimes torture. But the record, the financial records that you discover don't lie. They are diaries, they are confessions of which can save a populace, as was the case from a mass poisoning of ricin in the London subway system.

Indeed, when we read about the capture of Hambali several months ago, what was trumpeted was of course what we can learn from his interrogation. What was not trumpeted, and probably was more important than anything we are learning from his interrogation, is what was in his PC and what the PC contained in terms of his financial dealings.

Second, the ambition of a terrorist cell is defined by its resources, much like the ambitions of a business or a government. Moreover, the only link in the chain of terror that is subject to deterrence is the would-be banker who otherwise enjoys his anonymity and his affluence and his family's prominence. If he can be deterred—that is to be distinguished from the man who puts a bomb, straps a bomb on himself and walks into a marketplace, he is implacable, he is beyond redemption—but the banker who enjoys his anonymity, he can be stopped if he fears discovery and the loss of his freedom. If we can cut him short, we can cut the designs of terrorism short.

Third, no one is better suited to help police our financial borders than the financial services community and most of the folks on this panel. Indeed, the infinite number of ways that money can be spirited around the globe with the intention of killing people drives the need for more gatekeepers than this government has. That is in part the genius and in part the burden of Title III of the PATRIOT Act. To be sure, it is was and is at best a proxy for getting at a lethal challenge that we have never encountered before. I think, as I say later, it is very hard to judge the character of money. And in fact, when you talk to professionals to my left, it is characterized as a cliquesodic adventuresome idea.

And maybe it oughtn't be tried in a time of peace but we are at war, and if we don't try it, we abdicating the single most promising way to stop violence attributed to terror. Changing people's hearts and minds is a generational challenge. Stopping the logistical lines that fuels the terror, which is to say the money, is what we can do and what we should do and what our resources should be devoted to doing.

Now, there were great successes, as my testimony suggests, from the existence of the scrutiny at our financial borders, and my time is running fast. There are six specific suggestions I set forth in my testimony for continuing oversight by this committee. The most promising, I think, is the 314 safe harbor that has been established for discussions between one financial institution and another to do their own kind of scrutiny.

For whatever reasons, and perhaps the professionals to my left will tell us, I don't think that has borne the fruit it can bear. There are a host of other recommendations that I make—do I have—well, I had more time than I thought.

Chairwoman KELLY. Mr. Aufhauser, just go ahead and summarize. We are here to hear your testimony.

Mr. AUFHAUSER. Well, let me refer to this because it is constructive. I mentioned 314 and the dialogue that we ought to encourage between financial institutions to talk about suspicious activity. Similarly, the government has an obligation to share reciprocal information with the financial institutions. That has been devilishly difficult because to do so has a procedural hurdle, which is the se-

cure transmission of very sensitive data, and a substantive hurdle, which is you don't want to jeopardize ongoing investigations.

A lot of people are thinking about that. No one has found the panacea. Perhaps this committee can help, help examine that, so that the dialogue from government to financial institutions is complete and seamless and that we can be allied in guarding our financial borders.

We have yet to develop a topology for terrorist financing. I think it is because it is very difficult, but with all the intellectual caliber of the Silicon Valley and the financial community, I am convinced we can do it and that we have to have a war-like cabinet to make it happen.

Finally, very significantly, a lot of foreign countries have followed our lead in the adoption of anti-money laundering legislation, but it is at the wholesale level, as the finance minister of Pakistan said to me, "David, we need to take it retail, and we don't have the capability of taking it retail." So this committee should explore and urge a significant uptick in capacity-building, particularly in transitional economies about how to enforce and how to train people to enforce effectively anti-money laundering legislation and to combat terrorist financing.

I have more but I don't want to intrude on other people's time.

[The prepared statement of David D. Aufhauser can be found on page 34 in the appendix.]

Chairwoman KELLY. Mr. Aufhauser, thank you. I know you have more. All of your testimony will be in the record, and if we have time, I hope that the questions will bring out any testimony that you may be unable to give at this moment. But if not, I will probably go back and ask everyone to summarize again because this is a very important topic.

We move to you, Mr. Byrne.

STATEMENT OF JOHN BYRNE, DIRECTOR OF CENTER FOR REGULATORY COMPLIANCE, AMERICAN BANKERS' ASSOCIATION

Mr. BYRNE. Madam Chairman and members of the subcommittee, the ABA appreciates this opportunity to represent the committed men and women in the banking industry that work daily wit the USA PATRIOT Act on all of the laws covering the anti-money laundering obligations. When we last appeared before your subcommittee in March of 2003, ABA outlined a series of recommendations regarding needed areas of improvement to USA PATRIOT Act oversight.

We are pleased to report that a number of areas of concern have been addressed, and our partners in the government continue to work closely with the industry on needed improvements. We ask, however, that the regulatory agencies and law enforcement address several of the remaining 2003 recommendations.

In addition, ABA has two more recommendations. First, there needs to be a dramatic change in routine cash reporting under the Bank Secrecy Act so that there can be intelligent and efficient use of resources by both the government and the private sector in the continuing challenge of preventing our financial system from being used by criminals. Next, with the increased attention being placed

on risk-based compliance, the industry needs clear and concise guidance on suspicious activity reporting obligations.

Last year, we repeated our frustration that the Treasury Department had never fulfilled the 1994 statutory mandate to publish an annual staff commentary on Bank Secrecy Act regulations. As we stated at the time, "This indifference to congressional direction has contributed to industry confusion, examination conflicts and inconsistent interpretation of Bank Secrecy Act obligations."

We are pleased to report that FinCEN director, William Fox, has expressed his commitment to improved guidance through the use of advisories and commentary. We reiterate our promise to work with FinCEN and the appropriate agencies to achieve this overdue goal.

While we repeat our 2003 call that Congress ask the regulatory agencies to report on efforts in coordinating Bank Secrecy Act exams, we have seen a commitment to consistency in the past several months. For example, not only has FinCEN Director Fox expressed public support for uniform assessments, but he has also directed the Bank Secrecy Act Advisory Group to form a Subcommittee on Exam Issues. This subcommittee, co-Chaired by the ABA and the Federal Reserve Board, will review existing guidance and offer appropriate recommendations. We would be happy to report to this committee on our findings.

With the increased entities required to file suspicious activity reports, as well as the heightened scrutiny by regulators on SAR policies and programs, it is essential for the regulatory agencies, law enforcement and FinCEN to assist SAR filers with issues as they arise. This need is particularly obvious in the area of terrorist financing. As you heard from Mr. Aufhauser, this crime is difficult, if not impossible, to discern as it often appears as a normal transaction.

We have learned from many government experts that the financing of terrorist activities often can occur in fairly low dollar amounts and with basic financial products. Guidance in this area is essential if there is to be effective and accurate industry reporting. The bottom line is that terrorist financing can only be deterred with government intelligence shared with the financial services industry.

Recently, several financial institutions have contacted ABA about examiner criticisms received in reviews of their Suspicious Activity Report programs due, in large part, to the number of SARs that the institution has filed. These financial institutions expressed the concern, which we share, that the number of SARs filed meets a minimum threshold or that institutions are not filing the same number of SARs as peer institutions. The concern expressed is that there be new requirements in the form of a quota for determining the adequacy of SAR programs consisting, in large measure, of counting the number of SARs filed and, in some instances, comparing the number of SARs filed between peer institutions. Obviously, this would be a significant and alarming development in the examination and review process.

Moreover, regulatory scrutiny of SAR filings, and the recent civil penalty assessed against Riggs Bank for SAR deficiencies, has and will cause many institutions to file SARs as a purely defensive tac-

tic to stave off unwarranted criticism or second guessing of an institution's suspicious activity determinations. Obviously, if that continues, the legitimacy of the information in the SAR database will be called into question.

In terms of routine cash reporting, a February analysis by FinCEN shows that over half the CTRs filed would be eliminated if the current $10,000 threshold were raised $20,000 for businesses. The current dollar amount was created 35 years ago. While $10,000 is still a large amount of cash for individuals and probably should not be raised, reports on routine businesses simply clog the system.

Those who would argue that a change in CTR reports will lessen the banks' focus on cash transactions need to be reminded that the industry will still have reporting infrastructures in place, be required to file SARs on suspicious transactions and would retain the mandate to report individual CTRs over $10,000. We believe now is the time to adjust a process that is in sorely need of repair.

The ABA has been in the forefront of industry efforts to develop a strong public-private partnership in the areas of money laundering and now terrorist financing. This partnership has achieved much success but we know more can be accomplished. We commend the Treasury Department, the banking agencies and FinCEN for their recent efforts to ensure a workable and efficient process. We will continue our support for those efforts.

Thank you for this opportunity, and we will be happy to answer any questions.

[The prepared statement of John J. Byrne can be found on page 40 in the appendix.]

Chairwoman KELLY. We thank you for your testimony, Mr. Byrne.

Mr. Cachey?

STATEMENT OF JOSEPH CACHEY III, VICE PRESIDENT, CHIEF COMPLIANCE OFFICER AND COUNSEL, GLOBAL COMPLIANCE

Mr. CACHEY. Thank you, Madam Chairman and committee members. Western Union is a global leader in money transfer, and you are correct, we do business in 195 countries and territories around the world through 185,000 global locations. Internationally, over 70 percent of these locations are banks or national post office systems. Domestically, in the United States, we have over 45,000 locations which were made up of grocery store chains, convenience stores and check cashers, among other businesses. The important thing to note is that these are local businesses serving local communities' needs.

I just want to highlight three or four areas of my submitted testimony today in my opening comments. First, it is important for the committee to realize that from an anti-money laundering compliance standpoint, this is still a fairly new game to money services businesses. SAR reporting became a requirement for our industry at the beginning of 2002, and the Section 352 PATRIOT Act compliance programs went into effect the summer of 2002. So we are only 2 years in the process of educating an industry and getting an industry up to speed as to the responsibilities and how to do this right.

Our goal in working with our agents in the U.S. is twofold: First, education, and, second, to make it cost effective. From an educational standpoint, we have provided agents with turnkey compliance guidelines to get them up to speed as to something as simple as what does a compliance officer do? What do policies and procedures for anti-money laundering compliance program typically look like? What is employee education on these issues, and how do you document that? And then of course the internal reviews that need to occur.

We also provide our agents with ongoing regional training, topic-specific workshops and one-on-one training if they request it. And then we are currently and constantly enhancing these tools so that our agents are getting new information, information in a variety of languages, information that will allow them to build their programs and monitor their activities so they can fulfill the suspicious activity reporting requirement. We continue these efforts today and believe that the regulatory community should continue this effort in the same way.

Education is key. As a compliance officer, I tell my business clients, internal clients all the time that to start at ground zero and work your way to a full-fledged, mature compliance program takes 3 to 5 years. We have been scrambling to get it done in two to three ways, and I think we are well on our way, but we need to keep this in mind as we move forward.

Secondly, and a number of panel members have mentioned this, the regulations call for a risk-based approach, and we appreciate that. Industry and regulators should focus resources where the highest risk is actually located. In Western Union, for example, we treat different categories of our agents differently. We break agents down to national accounts, networks and independents, or what we commonly refer to in the industry as mom-and-pops.

A national account is typically a publicly traded corporation. They have internal legal departments, internal audit departments, typically you can start at the top, express what needs to be done for your particular service, and that could get pushed through to an organization in a very efficient manner. It takes less work to get a national account to do what needs to be done than any other account because they want to do it the right way.

Networks typically are regional. They also have internal infrastructures, if you will, but they typically need more help on the legal aspect: "What is BSA compliance, what is AML compliance, can you help us build our program?" But, again, once that program is built, they have good mechanisms and infrastructures in place to roll those programs out.

And then probably the greatest challenge is the mom-and-pops because they don't have access to lawyers readily, you don't want to make them hire a lawyer or a consultant to have to go figure out what the BSA is and how to build a program. They don't have a need for intense infrastructure within their business, and so you really need to walk them hand in hand through the process.

Western Union views this as a risk-based approach because each organization poses different levels of risk in getting programs rolled out, and we believe that FinCEN and the IRS should take

the same approach in applying their resources, both for education and then also the IRS' examination process.

Finally, I would just like to say a word on terrorist financing. As we have all indicated, today's terrorist cells strive to weave themselves into the fabric of our society to camouflage a financial legitimacy. Typically, they enter whatever jurisdiction they are entering into legally, they get valid government IDs, they get bank accounts, they get credit cards, they get debit cards, and, as we all know, we need a surprisingly small amount of money to do what they are striving to do. If a name gets put a public list, like the OFAC list, we will make sure that that person doesn't receive or send any transactions.

But the key is better non-public information, non-public intelligence from the government to let us know what should we be looking for? What are the government intelligence agencies seeing, what patterns are they seeing, what activities they are seeing so that we can look for that in our back room and identify that type of activity which is most useful to law enforcement.

Thank you very much for this opportunity, and I will be happy to answer any of your questions.

[The prepared statement of Joseph Cachey III can be found on page 50 in the appendix.]

Chairwoman KELLY. Thank you, Mr. Cachey. I was interested that you pointed out in your testimony that the terrorists can use rather discrete amounts of money in various ways, and I think that is an important piece of your testimony. I thank you for pointing that out.

Mr. Richards?

STATEMENT OF JAMES RICHARDS, OPERATIONS EXECUTIVE FOR GLOBAL ANTI-MONEY LAUNDERING, BANK OF AMERICA

Mr. RICHARDS. Thank you, Madam Chairman, Ranking Member Gutierrez, members of the subcommittee. As pointed out, I am the senior vice president and the global anti-money laundering operations executive for Bank of America. I held a similar position at FleetBoston Financial prior to the merger.

In both rolls, I have or had responsibility for the bank's operational aspects of preventing, detecting and reporting potential money laundering or terrorist financing. I stress, Madam Chairman, the operational aspects or operational perspective, as I bring to this subcommittee the perspective of someone who sees the Bank Secrecy Act and USA PATRIOT Act, the regulations and regulatory expectations and guidance firsthand and in operation.

From a purely operational point of view, money laundering and terrorist financing are two, very, very different problems. Traditional money laundering prevention is a transaction-focused internally sourced issue where transactions lead to relational links. Terrorist financing prevention is very different. It is a relationship-focused, externally sourced issue where relational links lead to transactions.

Take a typical money laundering case. We are required to detect and report potential structuring. Customers have come into the bank and structure cash transactions so as to avoid the large cash reporting requirements. Looking solely at those large cash trans-

actions is a pretty basic exercise and can lead to potentially suspicious activity but building a tool and having a program that enables you to take every customer who opens up an account without a taxpayer identification number, with an opening deposit of less than $100, who structures cash deposits in the United States and withdraws money through ATM machines in high-risk countries. Now, that is interesting and frankly is not that difficult to do.

Compare that typical money laundering case with a typical terrorist financing case. Almost every one of them starts with some sort of request from the government, whether it is a grand jury subpoena or a Section 314(a) information-sharing request. Let's say the request is for Bin Laden Enterprises, 123 Main Street. That would be a very typical 314(a) request. First, we have to scrub our various customer and transactional systems to determine if we have a match on that name.

Let us assume we don't have that customer at that address but we have Khalid Sheikh Mohamed and KSM Enterprises at the same address. We would have to then review our transactional systems, and we would find that KSM Enterprises sent wires to another entity called AQ Recruiting. We would use a surface web search engine, such as Google, to find more information on Khalid Sheikh Mohamed, KSM Enterprises and AQ Recruiting. Very often, even more important than what we find is what we do not find. Legitimate businesses generally cannot hide from the Internet.

We would also use what we call the invisible web resources such as Search Systems to find that Khalid Mohamed was an officer of both KSM and AQ, and there were six others that were officers of both. We may also find that those six were officers of six other companies. We then go back into our systems and perhaps find another 15 customers and 6 addresses that appear linked to all the people either transactionally or relationally. We would run those addresses and telephone numbers, and we would add more entities.

If one of our targets had a web site, let's say one of them is a charitable organization, we would then be able to go into the historical web and look at all of their web sites back as far as 1996. What we would have is something that was sourced by the government: even though it was not a match under 314(a), we would now have a case that involved at least 15 people, 10 companies transacting between themselves where the public information doesn't match their activity. And if the totality of the relationships and transactions led to a standard of suspiciousness, we then have a very effective and very good Suspicious Activity Report to file.

The success of the financial sector's anti-money laundering and terrorist financing prevention efforts is entirely dependent on two things: First, cooperation between and coordination by all of the parties involved: the law enforcement and intelligence communities, the regulatory community, the private sector, our trade associations, such as the ABA, and others; and, second, creative, committed professionals dedicated to this task.

In my experience, Madam Chairman, the American financial sector has both.

Thank you for this opportunity to testify on this very important topic. Bank of America remains committed to meeting its obligations of protecting, preventing, reporting and indeed mitigating the

effects of money laundering and terrorist financing and recognizes and applauds the efforts of its private sector colleagues and public sector partners in these efforts. Thank you.

[The prepared statement of James Richards can be found on page 72 in the appendix.]

Chairwoman KELLY. Thank you, Mr. Richards.

Mr. Emerson?

STATEMENT OF STEVEN EMERSON, EXECUTIVE DIRECTOR, THE INVESTIGATIVE PROJECT

Mr. EMERSON. Madam Chairman, members of the committee, I want to thank you for inviting me, and I also want to commend your for assembling a phenomenal panel this morning—the best panel I have seen on money laundering and counterterrorism issues. I also want to let you know, Madam Chairwoman, that I am very appreciative of the incredible leadership you have played the last 2.5 years since September 11 in terms of bringing to the attention of the American public, Congress, the media and other institutions the role that needs to be played by the private sector and government in fighting the scourge of terrorism.

I also want to express my appreciation to Congressman Royce who I have had the privilege of working with very closely following September 11 when Congressman Royce invited me to join his squatter's movement in various members' offices until they agreed to approve and support the PATRIOT Act. And I understand and appreciate very much what it takes to pass legislation in this great body.

I also want to let you know that I am very appreciative of my staff, Jon Levin and Dana Lessman, of the Investigative Project for their help in preparing this testimony.

One of the issues that we obviously would be looking at today in much greater detail, and are looking at, is the Riggs case. The question is does Riggs represent an exception or does it represent a pattern? Its failure to obey the order and file SARs, a suspicious activity report, in deference to the client's desire, principally that of the government of Saudi Arabia for secrecy, is the most single, serious breach every in the first line in U.S. history of financial controls against terrorism.

The bank officials who participated in these willful violations should be held personally responsible, and there are many questions that need to be answered. Whether clients are assured of a quid pro quo? How long did it continue to operate? To what activities have drawn funds from diplomatic accounts from Saudi Arabia at the Riggs branches? And considering the long-term problems with Riggs, why didn't the OCC consider it a high-risk institution?

I urge this committee to conduct a thorough and comprehensive review of the reports prepared by financial regulators and to work closely with law enforcement and financial oversight institutions to see exactly what went wrong in the Riggs case.

And although the Riggs case represents the failure of the financial sector in oversight, there are cases and examples that represent the courageous successes of institutions in helping to track and interdict possible terrorist operations. In this category, although he is very humble, my co-panelist, Jim Richards, I must tell

you, has played a singular role in helping and actually leading the government in identifying terrorists in the United States and helping to stop operations because of his recognition of actual activities in financial reporting that led the government to identify and issue law enforcement sanctions against possible terrorists.

Also, David Aufhauser has continued to play a leadership role in the war of terrorism financing. His vision and leadership is thoroughly needed as we move forward.

In one instance where I can discuss, and it has been publicly cited in previous reports, a major financial institution cut ties with a terrorist-linked bank after being advised to do so. In the year 2000 and 2001, Citigroup was participating in joint ventures with the al-Aqsa Bank, which has ties to Hamas. When informed by the Israeli government of those ties, Citicorp contacted the U.S. Treasury for guidance and subsequently terminated its relationship with al-Aqsa Bank.

So what is the true relationship and paradigm here? Is it Citigroup taking the initiative with the Treasury Department or is it Riggs Bank's failure to comply with the government mandates? Al Qaida and other terrorist groups have found huge crevices and holes in the financial structures of Western nations, exploiting not just their freedom of regulation but also the freedom of religion and freedom of thought, the freedom of expression to basically promote religious extremism under the guise of financial transactions.

That is something that necessarily financial regulators will not always be advised of or even be aware of, and in this case the concept advanced by Congressman Royce for a much needed financial intelligence ability, the creation of which is equivalent of having a CIA at Treasury that could recognize patterns, activities from those who established accounts to those who are the recipient, is absolutely critically needed for the first time in the war against terrorism.

Al Qaida itself has established its own banking system outside of European and U.S. law. Al-Taqwa Bank, for example, was created by the Muslim brotherhood in 1988 to move and safeguard large quantities of cash for terrorist causes. It was designated a terrorist entity by U.S. authorities in 2001. In January 2002, the Treasury deputy general counsel wrote to a Swiss prosecutor notifying that as of October 2000 Al-Taqwa seemed to be providing a clandestine line of credit for a close associate of Bin Laden. Reportedly, the Justice Department might now be close to bringing indictments.

The questions that you face in the future, and as you have faced in the last 2.5 years, is to what extent we can enlist and ensure that the private sector participates aggressively in the interdiction and recognitions of the dangers.

One very good statistic that I will tragically leave you with is the ratio of what the costs were to the damage of September 11. The costs of carrying out September 11 to the terrorists was about $500,000, largely in transfers of less than $5,000. The cost to the U.S. economy was $500,000 billion. That is a ratio, I don't need to do the match of a million to one. If we had spent a little bit more money ahead of time and invested it paying the price that we

should have paid, we might have been able to prevent this incredible tragedy.

Thank you, Madam Chairwoman.

[The prepared statement of Steven Emerson can be found on page 61 in the appendix.]

Chairwoman KELLY. Thank you, Mr. Emerson.

Mr. Aufhauser, there was a discussion in the April 20 Summit Banking Committee hearing about your suggestion of a separate examination and compliance force within the Treasury. In that hearing, there was some resistance from one of the witnesses, a head of one of the regulatory agencies. His resistance was based, first, on the idea that regulators should be given more time to prove that they can perform at the level that we expect in a post-September 11 environment. He went on to suggest that implementing new structural reforms would take time that we do not have.

I am very interested in your thoughts on these concerns. I think most of us would agree that we are in a new security environment for the long haul, but we should probably make sure that we have in place now a regulatory and compliance structure that will be capable of serving us all at a high level of effectiveness over a long period of time.

If we don't act now, aren't we just deferring legal reforms to a later date? And if, as suggested, I think we give the current regulators some time and we still don't reach the performance levels that we expect, then do we face the possibility of being in similar circumstances a couple of years down the road, having gained nothing during the way?

The Riggs Bank failed to report, the OCC failed to detect, this was something that I am wondering if it wouldn't happen again if we don't act now to do something. And I would be interested in what you have to say about that.

Mr. AUFHAUSER. Well, I can't divine whether if we had changed the structure, Riggs would have been discovered earlier, but what informed my testimony earlier, and I still endorse it, is two concerns. One is for uniformity. Two is without discounting in any way the professionalism of the folks at the OCC and the Federal Reserve, their larger mandate is safety and soundness when they take look at financial institutions.

AML issues and terrorist financial issues, which is a subset of AML in my judgment, are at risk. I am not saying it happens necessarily but are at risk of becoming stepchildren to the examinations. And in the best of all possible worlds, to quote, Penglas, I do believe it would be better to have one uniform compliance office that was enforcing the BSA regulations.

The second thing that informs that judgment is that the Treasury Department has relied on OCC and the Federal Reserve and indeed the SEC on delegating the authority and responsibility for examining compliance, because they are already heavily involved in the regulation of their industry actors. But the PATRIOT Act extended AML requirements to a whole host of industry sectors that do not have any coverage by any Federal regulator, whether it is casinos or whether it is insurers or whether it is car dealers and jewelry stores, and hedge funds, by way of example, also.

So there is a complete community of interest out there, which under 352 of the PATRIOT Act is responsible for complying and establishing AML programs, yet no one is policing them—no one, no one.

Chairwoman KELLY. That is really serious, and I think that it is something that we have got to—that is one of the reasons why we are having this hearing. I think it is very important that we move on with it.

I would like to ask both you and Mr. Emerson, should the new Undersecretary at the Office of the Treasury—that office is designated to coordinate anti-terrorist financial efforts. Should that office have the enforcement authority or should they just have intelligence capability and let the enforcement authority go to another agency?

And I would like to start with you, Mr. Aufhauser and move to you, Mr. Emerson.

Mr. AUFHAUSER. That is a hard question. That is a hard question because I haven't thought about it. I have always married the two interests, and I think it wildly inefficient not to have both. I do agree with what Steve said, and I am sure he will say more, we need a professional first-class, best-in-class financial intelligence unit in the U.S. government.

We have extraordinarily people populating various agencies of the government that pursue that interest. There is no one FIU right now, and there is no one woman or man charged with not only directing the resource application, directing the analysis but also holding people accountable. So that is a very important part of your question which is that there ought to be a very strong intelligence FIU unit.

What you do with that next in terms of enforcement, you used the word, "enforcement." It may not be enforcement. It may be other endeavors that you undertake, diplomatic or otherwise, to make sure that you are frustrating somebody's attempt to penetrate our financial borders to kill people.

I do think the person who possesses the best knowledge of the intelligence and who is charged with responsibility for establishing a strategy ought to be charged also with the responsibility for executing.

In the past, during my tenure, a lot of that was done by committee at the NSC, and although I think we did a really credible job, I do think the NSC is the wrong place to have an operational organization. It sets policy; it doesn't execute.

Chairwoman KELLY. Mr. Emerson?

Mr. EMERSON. I think you rightfully point out that the problem exists today. I remember reading the hearings, I think, last week or the week before, various officials in the Treasury as well as ICS where the number of three-and four-letter acronyms, I was dizzy by the time I read the third testimony. I think there were 19 I read and it was sort of like a Reuben Goldberg machine, and obviously there really wasn't some type of coordinating mechanism but there was a stovepipe relationship.

And I think your question goes to the heart of what is now being faced at the FBI, which is to the extent to which there needs to be a separate intelligence branch broken out of the FBI for enforce-

ment; that is let the enforcement people do the enforcement and let the intelligence people specialize the intelligence.

As much as I theoretically would like to endorse the notion of a combined enforcement and intelligence position, my feeling is that the intelligence people need to be thoroughly instructed, mandated and only focused on intelligence gathering. They have to live and breath it all the time. They have to work on an equal playing field, perhaps even in a higher playing field in terms of being able to mandate sanctions or enforcement, but there has to be a cadre.

As Congressman Royce has pointed out, the financial intelligence that needs to be created is only going to come from people. You can have the best software in the world, the best link analysis—I know that in our office we use Analyst Notebook, it is wonderful but in the end it is garbage in, garbage out—and it is only on the ability of people like Jim Richards to look at transactions in the actual account to say, "You know, there is something suspicious."

Last night I was reading over the actual transactions in the Sami Al-Hussayen case, that is the IANA prosecution that is being carried out in Idaho right now. And what was interesting to me I was looking over an 80-page matrix of financial transactions from his bank account over the last 2 years, and I was trying to figure out if I was a bank officer or a teller, could I have detected a pattern here of suspicious activity merely by looking at it.

If I look at the numbers, no, even though there are large numbers sometimes of $10,000, $15,000, $20,000 transfers within days of one another. But in terms of who was making the deposits and withdrawals in terms of either the Saudi cultural offices or Saudi government, this would have triggered something automatically, and it would have taken somebody who was read on to this and sensitized to this issue.

So I think to be comprehensive about it, a new undersecretary should be vested with everybody who reports to him on intelligence matters and I think actually have a position that oversees issues of enforcement.

Chairwoman KELLY. That is very interesting.

Mr. Richards and Mr. Cachey, I will start with you, Mr. Richards, but, Mr. Cachey, I want to go to you too. Can you identify any particular case in which your companies worked with law enforcement to stop the flow of funds to a terrorist group or an activity of some sort?

Mr. RICHARDS. Madam Chairman, off the top of my head, I can think at least two particular cases: One prior to September 11 and one after September 11. In both cases, we identified what we thought was suspicious activity. Again, we are not required to detect money laundering or terrorist financing, we are required to detect and report suspicious activity. We did that.

In both cases, we felt it was significant enough that we immediately contacted law enforcement, which we are entitled and indeed perhaps required to do if it is an ongoing, serious matter. And in this case, it was the Boston U.S. Attorney's Office, and they immediately contacted us and sought the underlying records that were the basis of our suspicious activity reports. Subsequent news events confirmed that what we had reported was indeed tied to potential terrorist financing.

Chairwoman KELLY. Mr. Cachey?

Mr. CACHEY. I think the important thing that I took away from Mr. Richards' comments was he discovered that they had done something wonderful through a news report, and I think that is the challenge we have. When we see suspected activity that we think is terrorist related, we report it directly to certain agencies within the government along with FinCEN, particularly Operation Green Quest when that was in effect and now Homeland Security.

But we don't get the type of feedback from law enforcement that we would like to get to say that SAR you filed or that phone call you made led to this activity. Because if you don't read about it in the newspaper, you really don't get any feedback, so we do have processes in place, both through our Compliance Department and our Security Department with several fellow agencies that we report suspected activity to, but feedback is hard to get, particularly if there is an ongoing investigation, which you can understand.

Chairwoman KELLY. Thank you both very much.

Mr. Gutierrez?

Mr. GUTIERREZ. Than you very much. I would like to thank all of the witnesses. It seems to me from listening to all the panelists that there are a couple of things that maybe we can improve on.

I kept hearing the phrase, "educating people," starting with you, Mr. Aufhauser, and others about who do we need to educate on our financial industries and how could we go about doing it better in terms of watching for suspicious activity and getting to it. Do we call them all in for—I mean they call us all in for meetings and I get educated on ethics rules and my staff does, and we get constantly—I know the doctors—good doctors will continuously get reeducated after. What do we need to do so that we can better do this?

Mr. AUFHAUSER. If I said the financial community needs to be educated, I only said half of what I intended to say. So does the government. I mean it really is a two-way street, and without the reciprocity, the exchange of the knowledge universe that each has, it is a fruitless endeavor.

I think what we have to educate each other on is getting smarter, ironically. My brief experience in my private life for the last 3 months has been there is actually overreporting of SARs, in part, simply out of a cautionary note by financial institutions and, in part, because with the exception of perhaps Jim Richards who seems to be very long on the tooth on what to look for, a lot of the new actors who are subject to SAR reporting don't exactly know what to be looking for.

Jim is exactly right, they don't file a SAR because they know it is terrorism and you don't file a SAR because you know it is a crime. You file a SAR because there is a suspicion, something to the character.

Mr. GUTIERREZ. I gathered that from your comments and from what Mr. Richards said. So is there a way of taking Bank of America and the kinds of things that we have heard here today and ensuring that other institutions do more?

Mr. AUFHAUSER. I don't know if it is that institutions need to do more. I just think we need to be smarter about what we are looking

for, and that requires what used to my office talking more to private industry.

Mr. GUTIERREZ. How do we——

Mr. AUFHAUSER. What we didn't have the genius, Congressman, and I didn't have the genius for is how do you do that without jeopardizing something incredibly sensitive? And I mean it in terms of broadcasting the information, sort of these 314 requests that go out and say, "Hey, this guy, Aufhauser, is suspicious. Do you have anything on him?" The most important dialogue I ever had with people like Jim or Joseph—and, by the way, there are stories one could tell about Western Union being terrific ally of the U.S. government in the war on terror which has nothing to do with capture but has everything to do with helping us abroad.

I think what we—you know, I have actually lost my train of thought there. What we need to be—the most productive thing I ever did was a specific targeted request for information because of a very sensitive piece of information. And I went to somebody I trusted in that institution. There was an element, a bond of personal trust. If we can figure out how to multiply that so that we can do more broadcasting of sensitive information, we will be more effective.

One last very soft observation: This is not about just capturing bad guys, it is about them fearing capture. And I have read plenty of intelligence, actually overheard intercepts where bad guys abroad said, "We can't use the U.S. financial banking system; they will catch us."

Mr. GUTIERREZ. And I guess what I have heard is maybe we are going to need to look into this a little further. And anybody who has any other comments on what we can do to better educate our folks and who we need to educate within that system that certainly, I think, would be helpful from your perspective. And, as you say, obviously we both need to educate each other. We need to do a better job on our side.

I have limited of time so I just want to—can we ask the other—thank you.

Mr. Byrne and Mr. Cachey, please.

Mr. BYRNE. Congressman Gutierrez, I want to make a couple of points about education. I don't want the committee leaving today thinking that there hasn't been for a good number of years a whole host of programs on big picture education, certainly, not just the laws and regulations but examples of money laundering cases once they are closed and the typologies that we share with bankers on what to look for going forward in the areas of money laundering and fraud and those sorts of crimes. So that goes on on a regular basis, and many of us participate in those sorts of programs.

I was at a program a couple of weeks ago on the west coast in which law enforcement, bank regulators and bankers met for 3 days and worked on terrorist financing and PATRIOT Act issues in which, for example, the IRS Criminal Division or the FBI would do a presentation on how a particular line of SAR reporting turned into a conviction, what to look for—while we don't have enough of these, what to look for in terms of terrorist financing going forward or money laundering.

Law enforcement does a very good job of doing training and programs. We in the industry need to be part of those as much as we can. We are not talking about investigations as they are pending, we are talking about once they are closed and we get some information going forward. So a lot of that has been occurring for the longest time that I have been at the ABA.

Mr. GUTIERREZ. I understand that. I mean I wish I had—I could take excerpts of what you have all said and either I am taking things out of context but I kind of heard here that we could do better.

Mr. BYRNE. Absolutely.

Mr. GUTIERREZ. So I don't want anybody to be defensive about what we are already doing well but what we can do better, and I kind of heard that we could do better from almost everybody, from Mr. Aufhauser all the way to Mr. Emerson. So from left to right, I heard we could do better.

So that is all I want to know is what we could do better. I understand that the institutions have done well and especially since we called this hearing because of what happened at the Riggs institution. So, obviously, Riggs would not be in the situation it is in today and Mr. Aufhauser said that the OCC and the Federal Reserve, which I agree with him, have safety and soundness as their basic mission. And they are expanding, the OCC is expanding its purview of what it decides it wants to do as a regulatory institution.

So, obviously, we could do better, and we want to be able to command those resources, and I think that is what this hearing is all about is to look at Riggs and how we move forward.

One last question, if I could, Madam Chair, and that is to the Bank of America and Mr. Richards. It seems to me you have harnessed common resources of the Internet and Excel to develop the systems to detect and prevent money laundering. What kind of compliance guidance have you gotten from your regulator regarding anti-money laundering efforts?

Was the system developed within your own institution or with the help from the government? Are you working together with us to develop the system at Bank of America or just by yourself in the private? How closely does your regulator monitor those activities? And how often do you hear back from the regulator after seeking—you file a SARs report, send them your report?: How often do you hear back from them, the regulators? That was a big question.

Mr. RICHARDS. I think it was perhaps four questions. I will try to answer them all.

Our program was developed at the former FleetBoston Financial. It was developed starting in January of 1999, and I often joked that it was two guys and two laptops, but that is exactly what it was.

What we did was try to build a—rather than build an anti-money laundering program, we tried to build a data management program. Our belief was that we needed to marshal all of the data and information that we had in the bank, and once we were able to marshal it, we could then look at it in a creative way for any purpose, whether it was money laundering or terrorist financing or marketing—any purpose.

As we developed that program our primary Federal regulators, which are the Federal Reserve and the OCC, monitored our development of that program literally on a continual basis. We met with them through our compliance partners in the bank on a quarterly basis, and they were very, very intrigued by it, not only because it was developed at a very low cost and used tools that people had on their desktops but hadn't before been using for anti-money laundering, but they were intrigued by the fact that it was a program that seemed to work reasonably well in a large institution but was applicable to the very, very smallest institutions.

And so the feedback we got was very, very positive. They were very, very interested in it, and indeed they have had me down to the FFIEC on I believe now four occasions to talk to the Federal bank examiners from all five agencies and tell them how we developed the program. And I know that John Byrne, the ABA, has directed other banks to speak with us, to see what we did and how we did it, and we have been sharing what we have done with every bank that is interested, which is a number of them. And I know that Western Union has also shown a great interest, and we have worked very closely with them as well.

So I think I have answered at least some of your questions. But, particularly, the OCC I think has been very, very interested in what we have done and how we have done it. And we are working very, very closely with them.

Mr. EMERSON. Mr. Gutierrez, if I could just add one thing here, because I think you have raised a very good point, and Mr. Aufhauser also raised the issue of sensitivity and information. Before September 11, the debate was always secrecy versus shared. After September 11, we realized that more people in the JTTFs and in law enforcement need to get intelligence, and the risks of having that information leak out was outweighed by the issue of having other people basically in line and aware of the threat and the information.

I think we should consider the possibility of certain bank institutions in need of certain thresholds to having designated officers that would be read on to certain classified information that they would be privy to information that is not made available just to the general public but made available to certain classified security programs, which they would be able to then use to help discern patterns in the larger context for transactions.

And, of course, there is always the risk of operational secrecy and leakage, but I think that would far outweigh the problems that would ensue if we didn't do that. So maybe that is something to consider to ensure that there is this financial intelligence of a nature that goes just beyond what the public stores documents, which, unfortunately, most of the time does not give a bank officer enough information to determine whether the transaction is sinister or not.

Mr. GUTIERREZ. Thank you. Thank you all for your service.

Mr. CACHEY. Madam Chairman, could I address that——

Chairwoman KELLY. Yes, by all means.

Mr. CACHEY.—just briefly? First, on the question of education, I think it is important from a money services businesses standpoint to realized that a number of the types of businesses that Mr.

Aufhauser mentioned before, the money transmitters, the pawnbrokers, the car dealerships, everybody that has become part of the PATRIOT Act family, if you will, are typically licensed and regulated at the State level.

So I think there needs to be greater cooperation between States that are licensing all these separate entities and the Federal Government and figuring out who is actually a money service business and should be having a program in place and reporting out on suspicious activity, and then coordinating those efforts between the Federal Government and the States.

Because right now you could have an IRS representative walk into your company and tell you X and then a State banking examiner from one of 47 different States come in and tell you why Z or A or B. And it is difficult, number one, to build consistent programs nationwide, but it is also difficult for the smaller MSBs to say who is correct here and what is the right thing for me to do because what we have discovered is we have worked through our agent basis.

Ninety-nine point nine, nine, nine percent of these business want to do the right thing, but they need somebody to tell them what is the right thing.

Mr. GUTIERREZ. You know something, I agree with you totally, and, unfortunately, we get results at the State level. Because when I try to reign in Western Union and Money Gram on the exchange rate, we could do nothing here in the Congress of the United States, but we could do things at the local level so that your exchange rate at Western Union is comparable to Mr. Byrne's Association of Bankers exchange rate. So I think we will have a difference of opinion on that.

Thank you very much.

Chairwoman KELLY. Mr. Hensarling?

Mr. HENSARLING. Thank you, Madam Chair.

Mr. Aufhauser, in your testimony, I believe you mentioned some anecdotal evidence of some intelligence intercepts where some of the bad guys were saying, "We have to steer away from the U.S. financial services system. It is not going to work for us." So I take that as very good news. As a former student of economics, I typically think in terms of cost and benefits. So the anecdotal evidence is persuasive but as a society what are we getting for all of these suspicious activity reports and the currency transaction reports? How do we measure success here?

Mr. AUFHAUSER. If you want to put a calculus on this, I have read studies that have suggested that the adverse consequence, that is the cost, of the World Trade Center is in the trillions of dollars. It wasn't just the loss of 3,000 lives, it wasn't just the disintegration of the buildings, it wasn't just the closing of our financial markets, but it was a market cap loss of an astonishing historic amount of money and the now daily tax, as I say in my testimony, that we all pay for enhanced security at virtually every door you pass through in America today. And that cost to me is almost incalculable and immeasurable, but it is certainly large.

So I measure that against—that is to say another calamity. If I measure the cost of another calamity, what it will do to our markets, our capital markets, what it will do to even more tightening

of what our freedoms are and more security cops and more machines and more taxes on the airline tickets and less freedoms, it strikes me that the cost and the burdens of a SAR compliance program are diminimus.

In addition, if you take it on a microeconomic level, every institution that is at risk of losing its good name, which is the principal asset any company has today because one errant transaction goes through there which is the cause of massive death, I think if you talk to many institutions, many of which are my clients, nothing is a higher priority than protecting their good name. And they don't measure it in dollars and cents.

Mr. HENSARLING. Mr. Emerson, part of your testimony, if I understood you properly, you said that most, if not all, of the financing of September 11 took place in financial transfers of approximately $5,000 increments. Did I understand you correctly on that point?

Mr. EMERSON. Yes. Most of them took—I think there were a couple of increments—not that all of this has come out or that I am privy to all of the transactions, but many of the transfers took place from banks, institutions in the Middle East, UAE, and transfers to corresponding accounts in the United States of $5,000 or less and then ATM transfers withdrawals of $300 or less by some of the September 11 hijackers.

Mr. HENSARLING. So right now if we have a $10,000 level on our currency transaction reports, in all probability those transactions would not be discovered in the system. Is that a fair assessment?

Mr. EMERSON. A $10,000 threshold would not have covered those $5,000 transfers, that is correct.

Mr. HENSARLING. Mr. Byrne, a question for you on the cost side of the equation. I was here last week participating in a hearing dealing with the regulatory burden on community banks. I represent the 5th Congressional District of Texas, which is kind of urban, suburban and rural, and we heard from a number of community bankers. For example, a banker in the city of Athens, Texas, a city roughly the size of 13,000. He was complaining about—and he wants to do his part as an American—the question of who reads all these reports, and is it doing good, and is it really worth the amount of money that I am having to put into the system in order to generate all these reports? Can you just very briefly tell us a little about your impression of the costs?

Mr. BYRNE. Well, first, I would just like to say in terms of the September 11 hijackers, those transfers that were mentioned were not necessarily cash transactions. So the CTR threshold issue really isn't relevant to whether we would or would not have caught those, because ATM withdrawals are not reportable today. You would have to have a suspicious reporting regime and looking at particular individuals.

But in terms of your question, I don't want to hang it on cost. I want to talk about policy, because, clearly, the small community bank does wonder about 13 million currency reports, the lion's share of those on Wal-Mart and JC Penny, what happens with those? And I would argue that even an IRS agent will tell you, "Not much." Suspicious activity reports, those are more subjective,

and certainly more goes into those reports, and I would argue that those are valuable, especially when we get the additional guidance.

So I think you have to look at the risk of a particular community bank and what type of response that institution has to have to make a determination whether they should have the same infrastructure as Jim Richards has at Bank of America. But the bottom line is we think you should focus more on suspicious reporting versus cash reporting, and that will help the small bank and the large bank if we make some dramatic changes there.

Mr. HENSARLING. Madam Chairman, I see I am out of time. Would I be able to ask one more question?

Chairwoman KELLY. Yes, please.

Mr. HENSARLING. Thank you, Madam Chair.

Mr. Richards, I believe in your testimony you stated that money laundering or terrorist financing is not a problem but a symptom of a problem. Could you elaborate and explain that statement?

Mr. RICHARDS. Yes. We believe that within the context of the total issue of operating risk, that the act of filing a suspicious activity report is not the end of your duty but indeed you take the suspicious activity reports and then you go back and look at the commonalities between them to determine whether the money laundering that you have reported or suspicious activity you are reported is caused by issues relating to account opening, failure to collect the proper identification, it might be a branch training issue where you have to train the people in the branch environment, something like that.

So that rather than looking at the end game being the filing of a suspicious activity report, you look at it as just the beginning of trying to see if there is an underlying operational issue in the bank. If you address the underlying operational issue, you may resolve the suspicious activity that is occurring in your bank. So, again, if you look at it as not a problem but a symptom, you can then drill down and see what the real underlying operational problem may be.

Mr. HENSARLING. Thank you.

And thank you, Madam Chair, for your indulgence.

Chairwoman KELLY. Thank you. We have been called for a vote.

Mr. Garrett, I am going to call on you, but I know Mr. Royce has very specific questions he would like to ask. So I will call on your Mr. Garrett, and then we will go—Mr. Royce, I know you have very specific questions you would like to ask, and with the indulgence of this panel, I would like to let Mr. Garrett go, we will then take a brief break and go to our vote, because it is apparently only one vote. We should be able to do that quickly and——

Mr. ROYCE. Could I inquire if we have 15 minutes, there might be time for Mr. Garrett and myself. He could go first and then I could follow up.

Chairwoman KELLY. Let's see what we can do.

Mr. ROYCE. Thank you, Madam Chair.

Chairwoman KELLY. Mr. Garrett?

Mr. GARRETT. Thank you, and I will keep it brief. There was an article in the American Banker publication with regard to the hearings that we had just a week ago and also the hearings that the Senate had, and I wasn't following the Senate hearings but they

were, and they said they saw a difference between the two panels. The House panel was raising some questions such as Jeff Seer, that I asked as well, with regard to some of the reporting requirements that maybe there is too much. Whereas the Senate hearings were sort of going in the opposite direction saying that failure of compliance is endemic, I think was the caption in the article, on behalf of the industry.

And nothing that I have heard so far or either one of the hearings indicates to me that there is an endemic problem as far as the industry is concerned. I am a little bit more concerned as to what we can do as far as the regulatory side of the equation. Mr. Gutierrez raised the point but we agree that a lot has been done already, some more, from your recommendations, can be done, and so I am just going to go along those lines very quickly.

Mr. Byrne, you raised the question, I would make a comment about the frustrations we have had over the time with the Department of the Treasury's failure to comply way after a 1994 mandate to publish an annual staff summary on the commentary on the Bank Secrecy Act. I don't know whether there are any repercussions on the Treasury Department for failure to comply. I don't know whether there are repercussions that had it been the other way around on the industry failing to comply with the Treasury Department, I have a feeling there probably would be.

Where are we now exactly on that? What is the explanation—because we don't have somebody here from them to ask—what is the explanation that we have had that we had a 10-year hiatus and failure to comply with congressional intent, as far as you are aware?

Mr. BYRNE. It is not clear that there is a proper answer to why there has been delay, but the good news, I believe, is that with the appointment of Mr. Fox at FinCEN, one of the first things that he said he would do is put together that long awaited commentary so that the industry could have the interpretations in one place so that both the regulators and the industry would have some place to go for some of those questions that are very difficult to discern for the local banker out in—you pick a place.

So from our perspective, we are trying to point out it has been there, it has been delayed, but we see some major progress, and we certainly have offered to work with them to communicate the final commentary or guidance when it comes out.

There have been some advisories, Mr. Garrett, in the past couple of years to give us some particular advice on certain issues, but it has not been enough. So we are very hopeful that Mr. Fox will come through with his commitment, and we are going to work with him and help him do that.

Mr. GARRETT. I am amazed, I guess, in a positive sense, by Mr. Emerson's testimony that last night or the last couple of nights you have been studying an 80-page matrix of these reports. There is nothing else that you would rather be doing at night than reading over these reports.

Mr. EMERSON. It is the life I live or the fact that this is the only thing that keeps me awake. And I would be happy to provide you a copy if you would like to see it.

Mr. GARRETT. Maybe your executive summary. I applaud that you do that, and I applaud that the industry has done that. I guess it is the overarching question as to where the dividing line comes as far as what the industry's responsibility is in these areas, and the suggestion has been made even as far as allowing some additional information, as far as security measures being woven over to the industry and how far we can go for that certainly for the large institutions and how far we can go for that as far as the smaller institutions as well. Can you comment as to how much of this burden can we actually place on the industry and where it should be laid best for the government?

Mr. EMERSON. Congressman, you raise an excellent question, and I don't know that I have the answer here, in part, because we haven't traversed this avenue before and in part because what has been done in the past hasn't really worked.

And I was speaking to a senior government official last night and I was asking him, "How can you expect a bank teller to make a determination that somebody is making a deposit and therefore triggering some type of—should trigger an investigation and report it?" And he says, "You are right, you can't really expect a bank teller to do that." On the other hand, the ability for someone like Mr. Richards or others who sort of have an inside intuitive nature because of their previous experience as prosecutors and the fact that they have good connections with law enforcement gives them an ability to discern patterns that ordinarily wouldn't accrue to somebody.

Now, you can't buy that off the shelf. It comes from hiring the right people, investing in the right people and making sure that the industry understands that people like Mr. Richards play a critical role in saving their institutions as opposed to sort of being a tolerated necessity that they have to endure as opposed to somebody that really should be brought in fully vested with as much financial resources as they can provide to give them that ability.

And, again, you raise an excellent question about what that dividing line is, and, unfortunately, it is impossible to discern it ahead of time.

Mr. GARRETT. And I thank all the members of the panel, and I am going to take this home and digest what you have said today. Thank you.

Chairwoman KELLY. Thanks, Mr. Garrett.

Mr. Royce?

Mr. ROYCE. Yes. I would like to go to Mr. Aufhauser and in my opening statement I talked about the need for better computer-aided efforts that would be used against terror finance, and right now the Financial Crimes Enforcement Network at Treasury has to depend on the IRS for its computer back office. No one I know thinks that the IRS is all that good with computers, and my question is would FinCEN be better at its job if it owned and operated its own computer systems?

Mr. AUFHAUSER. I actually don't think it is a question of hardware. It is almost irrelevant where the data is stored or the sophistication of the machine. I think it is the software. I think it is the need to have a dynamic technology platform that exploits the information as it rolls in. It answers both the question of trying to di-

vine, as difficult as it is, whether something is afoot, and it also in the longer run answers the question about whether these forms that get filed have utility and how to smarten both of those up; that is, the regulatory community and the regulator in terms of under what circumstances forms should be filed.

Going back to Mr. Garrett's question, it is, in part, burden, but it is also a genuine opportunity for each complying institution to participate in trying to know their customers and know the nature of the transaction that is ferreting through their institutions, because the risk to their reputation and their franchise is so great.

Mr. ROYCE. If Congress passed legislation that would create one key financial intelligence unit that would be housed in Treasury, that had appropriate powers, that had stature, not something in NSC but something really is given stature in Treasury, could that legislation be effective in solving the problem that we are talking about in terms of not only computer-aided efforts but the wider aspect of how you pull all the information together under one brain, under one controlling system that is able to analyze all of this?

Mr. AUFHAUSER. I am mindful of George Tenet's testimony before the 9-11 Commission when he said, "If you think establishing one single director of intelligence in this town is a smart idea, you don't know this town." You know, it is not the be all and end all but it is a necessary first step that is necessary but not sufficient.

I think it would be very important. There were literally times when I was told I was in charge of a theater of the war, and I responded, "I don't have troops." It would be better to have troops.

Mr. ROYCE. So that is a role that Congress, frankly, could solve. If we go, Mr. Aufhauser, to Mr. Emerson's testimony, one of the things he said in his printed testimony is permanent renewal of a strong and effective PATRIOT Act is fundamental to maintaining maximum pressure on the terrorisms advanced financial apparatus and machinations. And I would ask if you agree with that assessments?

Mr. AUFHAUSER. Yes. I am going to be parochial about this. With respect to Title 3 of the PATRIOT Act, absolutely. With respect to the broader content of the PATRIOT Act in terms of breaking down the wall, that is the ability of intelligence and law enforcement to talk to each other, and then Title 3, which breaks down the wall further of the ability of the government to talk to the financial community, it is absolutely essential.

If there is any lesson out of Madrid, if there is a lesson in the finance area out of Madrid, it is that every template that we have been looking at in the past for the financing of global terrorism, which is cross-border trafficking, is now actually betrayed. Because the financing from Madrid was local and pedestrian crime, as I said in my testimony. We need to marry cops with intelligence officials, with banks to stop the terror.

Mr. ROYCE. You mentioned the Hashish trade, you mentioned illegal immigration and how localities or whatever you would call them, they got information—they got funding through handling illegal immigrants that came across the border, and there was a third source of funding?

Mr. AUFHAUSER. Forged identity papers.

Mr. ROYCE. Oh, and the forged identity papers, again, used in immigration.

Mr. AUFHAUSER. What I call common crime.

Mr. ROYCE. Out of that they put the resources together that allowed them to organize and carry out that crime.

Mr. AUFHAUSER. They used it to purchase the explosives and to plan and to execute.

Mr. ROYCE. I would just close by asking Mr. Emerson if there is any other role for Congress here that you see besides what you have advanced in this paper that you would like to articulate, and then I guess we would better go and run and make that vote, Madam Chair.

Chairwoman KELLY. Yes. Unfortunately, because of the vote, I had expected to allow the panel some extra time to sum up anything that they had wanted to include in their testimony. I would ask you to do that in writing, please, because we haven't the time. So the Chair notes that some members may have additional questions for this panel which they may wish to submit in writing. So without objection, the hearing record will remain open for 30 days for the members to submit written questions to these witnesses and to place their responses in the record.

I am very grateful to all of you. You have been a wonderful, intelligent, very helpful panel. Thank you so much for sharing time with us today. This hearing is adjourned.

[Whereupon, at 11:41 a.m., the subcommittee was adjourned.]

A P P E N D I X

May 18, 2004

Statement of Chairwoman Sue Kelly
Subcommittee on Oversight and Investigations
"Improving Financial Oversight: A Private Sector View of Anti-Money Laundering Efforts."
May 18, 2004

An effective anti-money laundering system relies on a collaborative effort from the public and private sectors. This effort has received additional scrutiny recently due to problems at Riggs Bank, an instance where the public-private collaboration stumbled badly in protecting the public's best interest.

It is evident that the public and private sectors must continue to improve the way that suspicious activity is detected, reported and analyzed. Today we examine ways to improve the oversight and utilization of transaction information by regulatory and law enforcement agencies so the failures at Riggs are the last of their kind in our country.

The current enforcement structure we have put in place to enforce our anti-money laundering laws disperses various levels of responsibility through a convoluted group of Treasury bureaus and independent agencies.

While these agencies have been focused on efforts to oversee the safety and soundness of our financial institutions for decades, they must embrace new responsibilities which acknowledge that money-laundering is no longer a second-tier issue for financial regulators.

Of particular interest to this subcommittee are proposals to simplify the governmental structure so that regulation and compliance for these laws are better unified, perhaps even under the auspices of a single entity.

Given the vulnerabilities exposed by the Riggs case, I'm inclined to believe that the current structure is a relic of a foregone era and that substantive organizational reforms are necessary.

At a bare minimum, Congress should begin now an active and thorough assessment of proposals aimed at strengthening our enforcement regime. This subcommittee intends to do just that in the coming weeks and months, and therefore I look forward to testimony from some of our witnesses as to how we might significantly improve the effectiveness of our system without creating yet another layer of bureaucracy.

Our financial regulators must place a strong emphasis on compliance through rigorous oversight, taking swift and forceful action for non-compliance when necessary. This oversight includes working with the private sector to develop accurate risk assessments that enable examiners to focus on specific institutions, because resources need to be concentrated appropriately.

The continued leadership of the Administration and the Treasury Department is essential to improving financial oversight. Earlier this year, President Bush signaled his commitment to the war against terror by proposing a 14 percent increase in funding for the Financial Crimes Enforcement Network. FinCEN plays a key role in efforts to stop financial crimes by working with the financial community and supporting local, state and federal law enforcement and intelligence agencies.

The Administration has also announced the creation of the Office of Terrorism and Financial Intelligence (TFI) within the Department of the Treasury to unify, under one structure, the functions of several offices. I applaud the Administration for its efforts to streamline and centralize our anti-money

laundering efforts. There must be greater communication between FinCEN, law enforcement, the banking regulators and financial institutions, and I believe this office was an important step toward improving this coordination.

Now we must work to bring the next steps into focus. As evidenced by the failures of Riggs Bank and its regulator, the OCC, it is time to explore further reforms that improve the overall structure of our anti-money laundering efforts.

It is unacceptable that a Washington, D.C.-based bank with the largest embassy banking clientele allowed tens of millions of dollars to pass unnoticed and unreported through accounts belonging to Saudi Arabian government officials.

This activity continued even after a consent order was put in place last year. The mechanisms we put in place to detect and report suspicious activity failed – repeatedly. We no longer live in a world where such failures can be tolerated.

I thank the witnesses for appearing here today. You are on the front line of these efforts, and I look forward to hearing your views on how we can continue improving financial oversight.

Testimony of David D. Aufhauser
Senior Counsel at the Center for Strategic & International Studies
and Counsel to the Law Firm of Williams & Connolly
Before the
House Financial Services Subcommittee
Oversight and Investigations
May 18, 2004, 10:00 a.m.
The United States House of Representatives

Chairman Kelly, Congressman Gutierrez and distinguished members of the Committee, thank you for inviting me to address the issue of improving oversight of the integrity of the domestic and international financial systems. The subject is central both to efforts to frustrate, identify and eliminate criminal wrongdoing and to make it plain hard, if not impossible, for our financial borders to be penetrated by terrorist design and purpose.

Probably one of the most vexing issues you face today as members of this Committee is the unprecedented nature of the threat of terrorism. The DNA of war has, in fact, changed inalterably. Confirming the asymmetric power of our military, no sentient force confronts the United States on a conventional battlefield with a uniformed army under recognized flag. Nor is there a finite list of strategic targets to bunker with concrete and steel. Rather, the highest of profile targets are said to be "soft," open to the most outrage and the most unspeakable scenes of mayhem and despair – a school bus, a marketplace, a monument, a place of worship, and even these very halls.

The greatest infamy, of course, in this uncommon war is the premium placed on the death of innocents. Bullets and boots on the ground will not alone protect us. This is shadow warfare and it requires a "rethink"or a reengineering of what it means to defend a nation.

Every element of national power must be brought to bear, even the finance ministry of the United States, as anomalous as that sounds. With so many targets that defy military purpose and, therefore, escape common measures of detection, the three most critical factors that emerge are (i) the need for enhanced intelligence, (ii) the leveraging effect of disrupting the logistical lines that constitute the purchase for stealth and the export of terror, and (iii) the need for citizen soldiers and, in particular, a genuine partnership between business and government.

The funding of terror is the one common denominator in all three theorems. **First**, it is virtually the only intelligence that has true integrity in this war. All other information is suspect, the product of bribery, deceit, custodial interrogation, betrayal or, even in some cases, torture. But financial records do not lie. They are diaries, the confessions of which can save a populace – as was the case – from a mass poisoning of the London subway system.

Second, the ambition of a terrorist cell is defined by its resources. Moreover, the only link in the chain of terror that is subject to deterrence is the would-be banker who otherwise enjoys his affluence, his family's prominence and his freedom. If he is deterred, the reach of terrorist design is cut short, as is the quotient of violence in the world.

Third, no one is better suited to help police our financial borders than the financial services community itself. Indeed, the infinite number of ways that money can be spirited around the globe with the intention of killing people drives the need for more gatekeepers than government possesses.

That is part of the genius and part of the burden of Title III to the Patriot Act. To be sure, it is and was at best a proxy for getting at a lethal challenge that we have never encountered before. It has, accordingly, been administered in a manner that permits maximum discretion and that asks each relevant industry actor to identify the kind of risks that are unique to their enterprise.

Three consequences flow from that character of governing: substantial freedom to determine what is required of you; uncertainty because it isn't cast in stone, yet can have legal consequence of profound reputational impact; and genuine human interest in determining whether this all has real world consequence.

The latter is indisputably the case. The correct question is not who we have caught, but rather who has declined to move forward with terrorist design for fear of detection. During my tenure at Treasury and the NSC, there was ample intelligence that the enhanced scrutiny warded off acts of terrorism.

What is less certain is whether we have made the most out of the Patriot Act. Five issues merit examination by this Committee:

(i) Section 314 establishes a safe-harbor for financial institutions to share suspicions about counter-party accounts and matters. Perhaps because it is new, or perhaps because of appropriate conservatism about sharing confidential financial information, the utility of this private party sleuthing has not born full fruit.

(ii) Section 314 similarly permits government to share material information with its gatekeepers. Yet this discourse has been similarly abbreviated, principally due to

security concerns that are both procedural – secured lines of communication – and substantive – prejudice to an on going investigation due to premature disclosure.

(iii) Much of the information that is submitted to the government under the Bank Secrecy Act is merely lodged like a book on a library shelf without a card-catalogue. In the absence of an express and pointed request from law enforcement, the information remains unexploited. Surely, we ought to have an artificial intelligence program that red flags patterns and concerns for investigation without specific targeted inquiry.

(iv) Too few meaningful topologies of terrorist financing have been developed that can be models for suspicious activity triggers. In an age of Silicon Valley and extraordinary sophistication in the financial community, this particular missing ingredient screams for remedy.

(v) Section 311 is, perhaps, our most promising tool for impacting foreign banking institutions to exercise appropriate degrees of scrutiny. Treasury has a promising program focusing on such foreign "bad banks" and it ought to be encouraged by this Committee. The § 311 power is extraordinary and can effectively undercut the franchise of an international banking institution.

(vi) Many foreign countries, following our lead, have adopted templates for anti-money laundering legislation and terrorist financing initiatives. Particularly in transitional economies, these countries need training and resources to enforce what they have adopted as law. To quote one the finance minister from Pakistan in a meeting with me shortly before I left office, we need to go "retail" – that is, bring the knowledge of the law and suspicious trading to the street level.

The Riggs-Saudi accounts put the matter in high relief. One of the things that threaten us most is not money expressly earmarked to underwrite a specific act of terror, but the rivers of money that flow throughout the Islamic Diaspora to fund the teaching of intolerance and hate. It is that money that ignites tinderboxes and serves as a crucible for the alchemy that morphs intolerance into terror. Identifying and stemming the flow of those funds is the challenge with the most far-reaching consequence, and one that requires a rich and complete sharing of information between government and private industry.

Virtually all of my talk has been about terrorism. But the lesson of Madrid confirms an unholy alliance between common pedestrian crime and money laundering and acts of terror that can literally topple governments. The Madrid funding apparently was sourced from the sale of hashish, the forgery of false identity papers and the smuggling of aliens into Spain and Europe.

This is crime that not only corrupts, but kills. And it is crime that affirms the wisdom of the Patriot Act in taking down the "the wall," the barrier that muted all dialogue between intelligence and law enforcement, thereby savaging any hope of an integrated response to threat. The Patriot Act, in fact, takes that one step further, permitting an open dialogue between government and the financial services community. The challenge to the Treasury Department and this Committee to find a key that finally unlocks that door of reluctance to establish a financial intelligence source that is both a safety net and weapon against the killers.

The long-term war against terrorism requires a change of hearts and minds. But we need not wait for that generational challenge to succeed. The immediate hope for a respite against terror is tracing and stopping the money.

Al Qaeda tried to use commerce to destroy commerce, leveraging the loss of 3000 lives with catastrophic economic loss and in the daily "tax" that we all pay for heightened security at every door through which we now pass. An effective use of our financial regulatory structure can make those doors swing more freely.

One last note. I do not want to sound Pollyannaish. The President's war on terror has had a devastating impact on the hierarchy and banking network of Al Qaeda. But the organization is more movement than enterprise today. It has given birth to a hundred cancers, some characterized by simple nihilism, others by a political desire only to demonstrate the limits of U.S. power. Allied with local crime fronts, they pose with some irony even more threat to our well being than the monster we faced on September 11. The sheer number and diversity of our enemies underscores the continuing need for vigilance at the financial borders and the wisdom of enlisting the financial community in the war. Trying to figure out the character of money is quixotic in a world of peace. It is critical in a world of war.

Testimony of

John J. Byrne

On Behalf of the

AMERICAN BANKERS ASSOCIATION

Before the

House Financial Services Subcommittee on Oversight and Investigations

On

"Improving Financial Oversight: A Private Sector View of Anti-Money Laundering Efforts"

May 18, 2004

Madam Chairman and members of the Subcommittee, I am John Byrne, Director of the Center for Regulatory Compliance with the American Bankers Association. The American Bankers Association appreciates this opportunity to discuss how the financial industry is addressing compliance with the USA PATRIOT Act and all of the laws covering anti-money laundering (AML) obligations.

The ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country. For further information regarding the ABA, please consult the ABA on the Internet at http://www.aba.com.

The ABA and our members continue to work with our government partners in training financial institution employees on detecting and reporting the myriad of financial crimes that involve money laundering and terrorist financing.

Among other things, the Association holds an annual conference with American Bar Association on money laundering enforcement, produces a weekly electronic newsletter on money laundering and terrorist financing issues, offers on-line training on Bank Secrecy Act (BSA) compliance requirements, and has a standing committee of over 40 bankers who have AML responsibilities in their institutions. In addition, we have provided telephone seminars on compliance with Section 326 of the USA PATRIOT Act and AML examination issues. We will also address the nuances of the suspicious activity reporting requirements later this summer. The industry's commitment to deterring money laundering continues unabated and we have trained hundreds of thousands of bankers since the passage of the Money Laundering Control Act in 1986. [1]

When we last appeared before your subcommittee in March 2003, ABA outlined a series of recommendations regarding "needed areas of improvement to USA PATRIOT Act oversight." We are pleased to report that a number of areas of concern have been addressed and our partners in the government continue to work closely with the industry on needed improvements. We ask, however, that the regulatory agencies and law enforcement address several of the remaining 2003 recommendations.

The American Bankers Association has two additional recommendations. First, there needs to be a dramatic change in routine cash reporting under the Bank Secrecy Act (BSA) so that there can be intelligent and efficient use of resources by both the government and the private sector in the continuing challenge of preventing our financial system from being used by criminals. Next, with the increased attention being placed on "risk-based" compliance, the industry needs clear and concise guidance on suspicious activity reporting (SAR) obligations.

As we approach the three-year anniversary of the passage of the USA PATRIOT Act, now is the time to focus on how best to achieve the goals shared by all of us --- a strong and secure financial system.

---

[1] A 2003 survey by ABA Banking Journal and Banker Systems Inc. found that Bank Secrecy/AML/OFAC was the number one compliance area in terms of cost in the banking industry. It is also interesting to note that in banks under $5 billion in assets, 75.6% of the employees said that compliance was not their only job.

Our statement today covers the status of the 2003 recommendations, as well as a caution regarding what occurs with a lack of consistency in "Anti-Money Laundering (AML) and PATRIOT Act" examination procedures on what constitutes an appropriate SAR program.

In 2003 ABA recommended:

- Creation of an office for USA PATRIOT Act oversight;
- Immediate development of a Staff Commentary for PATRIOT Act and Bank Secrecy Act interpretation;
- Review of the 314 Demands for Record Searches;
- Formal commitment from **all** functional regulators for uniform and consistent PATRIOT Act exam procedures;
- Coordination between the Treasury's Office of Foreign Assets Control (OFAC) and the financial institution regulators to improve advice to the regulated community; and
- Improved guidance and communication on all SAR related issues, particularly in the area of terrorist financing.

In addition to the above, the American Bankers Association strongly recommends:

- Clarify that Financial Institutions are NOT required to file a specific number of SARs in order to have a compliant SAR program, and
- Raising the threshold for filing "Currency Transaction Reports" (CTRs) for corporations and businesses from over $10,000 to over $25,000;

Goals of an Office of USA PATRIOT Act Oversight Can Be Achieved Through Existing Mechanisms

Since we advocated that the Treasury Department create a formal mechanism for responding to questions concerning interpretation of PATRIOT Act obligations, a new Director has been appointed to the Financial Crimes Enforcement Network (FinCEN). William Fox has impressed the industry with his immediate commitment to both enhancing industry-government partnerships and to provide guidance on PATRIOT Act and AML issues. Therefore, we believe that our recommendation that there be "an office within the Treasury to communicate guidance, interpretations and FAQs regarding all PATRIOT Act questions" can be achieved through the new leadership at FinCEN. ABA also believes that the Treasury's Executive Office for Terrorist Financing and Financial Crimes will continue to provide value in offering guidance in addressing the ambiguous requirements of reporting terrorist financing.

FinCEN's Announced Commitment to a Bank Secrecy Act Staff Commentary

Madam Chairwoman, last year we repeated our frustration that the Treasury Department has never fulfilled the 1994 statutory mandate to publish an annual staff commentary on the Bank Secrecy Act regulations (Section 5329). As we stated at the time, "This indifference to congressional direction has contributed to industry confusion, examination conflicts and inconsistent interpretation of Bank Secrecy Act obligations."

We are pleased to report that Director Fox has expressed his commitment to improved guidance through the use of advisories and commentary. We reiterate our promise to work with FinCEN and the appropriate agencies to achieve this overdue goal.

The Improvement of the Section 314 Demand Process

The American Bankers Association was severe in our criticism of the implementation of Section 314(a) of the PATRIOT Act. The 314 process requires financial institutions to search accounts for potential matches to names on government investigative lists. As you may recall, many of our members complained that despite the clear congressional direction to the agencies, there was no apparent connection to terrorism or money laundering in the demands. Instead, the "requests" seemed to be a dumping ground for law enforcement cold cases.

Since that time, the regulators, law enforcement and Treasury made adjustments and the process was revised to "address a number of logistical issues and to develop additional guidance on the information request process."

The announced changes included the following:

- 314(a) requests from FinCEN will be batched and issued every two weeks, unless otherwise indicated in the request.
- After receiving a 314(a) request, financial institutions will have two weeks, rather than one week, to complete their searches and respond with any matches.
- Searches will be limited to specific records and, unless otherwise noted, will be a one-time search.
- 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 changes have been instrumental in improving the process. While we still have concerns that law enforcement does not always respond promptly to contact from financial institutions on matches, the overall consensus is that 314 is a vastly improved process.

Uniform and Consistent PATRIOT Act/BSA/AML Examination Procedures

ABA has previously emphasized that the banking agencies need to reach agreement on how the financial services industry will be examined for compliance under the PATRIOT Act and the other AML requirements. As we indicated at the time, "too often, institutions of the same approximate size, in the same geographic area and offering the same financial products are treated differently for compliance purposes. This should not continue."

There have been recent examples of coordination of examination procedures by the agencies but the process is not complete and there are some outstanding issues. We will discuss one glaring problem --- assessment of the adequacy of SAR programs, later in this testimony.

While we repeat our 2003 call that Congress ask the regulatory agencies to report on efforts in this area, ABA has seen a commitment to consistency in the past several months. For example, not only has FinCEN Director Fox expressed public support for uniform assessments, but he has also directed the Bank Secrecy Act Advisory group (BSAAG) to form a subcommittee on examination issues. This subcommittee, co-chaired by the ABA and the Federal Reserve Board, will review existing guidance and offer appropriate recommendations. We would be happy to report to this Committee on our findings.

OFAC and the Regulated Community

ABA pointed out last year that the compliance obligations under the laws administered by the Treasury's Office of Foreign Assets Control (OFAC) is a major requirement for the industry. One of the many concerns is what constitutes adequate compliance?

For example, the answer to one of the most common questions "Does OFAC itself require that banks set up a certain type of compliance program?" gives the industry little solace. The answer, according to OFAC, is that OFAC is not a bank regulator and the institution should check with their regulators "regarding the suitability of specific programs to their unique situations."

Madam Chairwoman, ABA and our members still need improved direction from both OFAC and the bank regulators on what is considered an acceptable OFAC compliance program as well as a reasoned analysis on the scope of these requirements. The banking agencies are preparing examination procedures in this area and we hope that the process will shed some light on the industry obligations with the 27 programs administered by OFAC. ABA is planning an OFAC Summit for sometime in July and we will report to the Committee on any outstanding issues.

SAR Guidance

With the increased entities required to file suspicious activity reports (SARs) as well as the heightened scrutiny by regulators on SAR policies and programs, it is essential for the regulatory agencies, law enforcement and FinCEN to assist Suspicious Activity Report (SAR) filers with issues as they arise. This need is particularly obvious in the area of "terrorist financing." This crime is difficult, if not impossible, to discern as it often appears as a normal transaction. We have learned from many government experts that the financing of terrorist activities often can occur in fairly low

dollar amounts and with basic financial products (e.g. retail checking accounts). Guidance in this area is essential if there is to be effective and accurate industry reporting. The bottom line is that terrorist financing can only be deterred with government intelligence.

For money laundering and other financial crimes, government advisories and other publications are a critical source for recognizing trends and typologies. As our Association pointed out in a 2003 comment letter on the "suspicious activity report," the interagency-authored publication, the **SAR Activity Review**, often includes a number of examples of activities that represent reported financial crimes. This information is extremely useful for training purposes. As the private sector co-chair of the **SAR Activity Review**, I can assure you the ABA supports the efforts of FinCEN and the participating agencies in crafting a publication that provides necessary statistical feedback to the SAR filing community. The **SAR Activity Review** has provided a variety of examples of the characteristics of such diverse suspicious activity as identity theft, bank fraud and computer intrusion.

We are pleased that the upcoming edition of the **SAR Activity Review** will provide, for the first time, the summary characterization of all of the suspicious activity categories. This should assist filers in advancing their understanding of the reporting requirements.

The Number of SAR filings should Not Be Determinative of an Adequate SAR Program

As stated above, there is one major problem affecting banks in the AML exam process. Recently, several financial institutions have contacted ABA about examiner criticisms received in reviews of their Suspicious Activity Report (SAR) programs due, in large part, to the number of SARs that the institution has filed. These financial institutions expressed the concern, which we share, that this may reflect new criteria for evaluating the adequacy of SAR programs, namely, that the number of SARs filed meets a minimum threshold, or that institutions are not filing the same number of SARs as "peer" institutions. The concern expressed is that there be new requirements in the form of a "quota" for determining the adequacy of SAR programs consisting, in large measure, of counting the number of SARs filed and, in some instances, comparing the number of SARs filed between "peer" institutions. Obviously, this would be a significant and alarming development in the examination and review process.

It is without question that the continuing importance for filing SARs is to inform governmental authorities of the existence of suspicious activity that may merit further investigation by law enforcement or supervisory agencies. As was stated recently by FinCEN is the "Guidance on Preparing a Complete and Sufficient Suspicious Activity Report Narrative":

The purpose of the Suspicious Activity Report (SAR) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA). In many instances, SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations and other criminal cases. Information provided in SAR forms also presents the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) with a method of identifying emerging trends and patterns associated with financial crimes. The information about those trends and patterns is vital to law enforcement agencies and provides valuable feedback to financial institutions.

Concurrently, one of the primary, if not the most significant, reason for institutions to have adequate SAR programs is to ensure that potentially suspicious activity is appropriately identified and managed within an institution. The adequacy of a SAR program cannot be judged by the number of SAR filings, but rather must be evaluated with regard to the institution's ability to identify potentially suspicious activity, evaluate whether the activity rises to the level of being suspicious requiring the filing of a SAR and, ultimately, lead to a process to determine how the activity is dealt with within an institution.

The notion that the number of SAR filings can determine the adequacy of a SAR program is, by all accounts, faulty. Clearly, an institution that has not filed SARs or has a track record of minimal filings deserves closer scrutiny of its SAR program, as it may be indicative of problems within that program. However, the lack of filings or the limited number of filings should be nothing more than a signal to the supervisory agency that a closer review of the SAR program is warranted. A determination of this type should be the result of a comparison of the number of filings of a particular institution against that institution's pattern of SAR filings rather than a comparison of filings between institutions. As an example of focusing on a particular institution's SAR filings rather than comparing filings between institutions, the Federal Reserve Board instructs its examination staff to:

. . . continue the process of assuring that SARs are reviewed prior to the commencement of an examination or inspection. As the Reserve Banks have learned, a pre-examination/inspection review of SARs assists the supervisory staff in assessing compliance with the SAR requirements and provides useful information regarding potential problems that may require special attention during the course of an examination or inspection.

Variations in the number of SAR filings between like or peer institutions can be attributed to numerous factors and, therefore, is not itself a reliable indicator of the adequacy of a SAR program. The type of customer base that an institution maintains (for example, retail vs. corporate clientele), the markets in which an institution operates or differences in the parameters applied in monitoring customers and their transactions are all factors that may lead to wide variations in the numbers of SAR filings between institutions. Additionally, contrary guidance or direction provided to institutions by the particular functional regulator of an institution can have a significant impact on the way in which an institution views suspicious activity, affecting the number of SAR filings between institutions. (For example, several financial institutions have reported to the ABA that examiners have instructed institutions to file SARs if they believe that they have information that may be of interest to the government, such as identifying an account or transaction related to an investigation that has appeared in the press, without regard to whether suspicious activity actually exists.)

Moreover, regulatory scrutiny of SAR filings (and the recent civil penalty assessed against Riggs Bank for SAR deficiencies) has and will cause many institutions to file SARs as a purely defensive tactic (the "when in doubt – file" syndrome) to stave off unwarranted criticism or "second guessing" of an institution's suspicious activity determinations. Obviously, if that continues, the legitimacy of the information in the SAR database will be called into question.

The SAR process should be addressed as the Federal Deposit Insurance Corporation (FDIC) examination procedures cover the area, by explicitly recognizing that there may be a variety of legitimate reasons for variations in the number of SARs filed by the same institution:

Determine if the institution or any branches had significant changes in the volume or nature of SARs filed, and investigate the reason(s) for these change(s). . . (Note: Increases in SARs may be caused by an increase in high-risk customers, entry into a high-risk market or product, or an improvement in the bank's method for identifying suspicious activity. Decreases may be caused by deficiencies in the bank's process for identifying suspicious activity, the closure of high-risk or suspicious accounts, personnel changes, or the failure of the bank to file SARs.)

With the increased focus on SAR programs and the number of SAR filings by institutions, the financial services industry is becoming increasingly concerned about the regulatory review of the SAR process. We believe that there is no correct number of SARs that should be filed in order for a determination that an institution has an adequate SAR program. A comparison between institutions of the number of SARs filed is wrong. It would be helpful if the government would re-state that SAR reporting obligations are based on an institution's analysis of potentially suspicious activity. If an institution has a SAR program that allows for a reasoned analysis of potentially suspicious activity and the institution's program is being followed, there should be no need for discussions regarding numerical threshold of SAR filings and no comparisons between institutions. Madam Chairwoman, the need for SAR guidance must be a major priority and we appreciate the fact that the BSAAG is also looking at these types of issues.

One final point concerning the validity of the suspicious activity reporting process concerns the chilling effect that has resulted from the massive leaks of SAR reports to the media. SARs are confidential documents, prepared after careful analysis, designed to trigger law enforcement investigations. SARs, however, are prepared by financial institutions not law enforcement officials. SARs do not always lead to investigations, let alone convictions. The very real fear that a SAR may appear in print will certainly impact the reporting process.

It is completely unacceptable and potentially criminal for those documents to have been disclosed to major news outlets. We applaud Director Fox for his public condemnation of these actions and urge swift action against the perpetrators.

Cash Reporting --- A Major Change is Warranted

It is clear that there are only a finite amount of resources available in both the government and the private sector to address financial crime. Certainly, the most important report filed by the industry is the Suspicious Activity Report (SAR).

Reporting apparent crime is superior as an investigative tool to routine reports of cash deposits or withdrawals over $10,000. The cash reporting requirements were the result of the Bank Secrecy Act, a 1970 law (PL 91-508) created "to require certain reports or records where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." The BSA is a reporting and recordkeeping mandate that, in general, requires the filing of currency transaction reports (CTRs) for cash transactions over $10,000. This statute has been costly for the industry to implement, but we acknowledge that it has achieved some success in the money laundering prevention area. Whether or not the benefits have been worth the resource allocation is an issue that has never been adequately addressed.

As far back as 1993, I authored a law review article on the subject of BSA burdens on our industry and their relative lack of utility. I pointed out that the BSA regulations have not always been

consistent with the 1970 goals mentioned above, and that subsequent changes to the Act "have resulted in a patchwork of regulations and laws that have saddled financial institutions with many responsibilities" that have "never been subject to any thorough analysis of whether they have (or will) fulfill the intended purpose of the BSA."[2]

Congress and the agencies also believed there was a need to change how cash transactions were filed and as a result, passed the 1994 Money Laundering Suppression Act. This law received widespread support, in part, because of the Congressional concern that routine CTRs "are expensive for financial institutions to file and for the Treasury to process, and [they] impede law enforcement by cluttering Treasury's CTR database."[3]

The 1994 statutory changes to the CTR reporting system were finally implemented by Treasury's Financial Crimes Enforcement Network (FinCEN) in 1998, and financial institutions may now reduce, to a one-time filing, cash reports of many retailers, governmental agencies and other legitimate entities. Since banks file millions of routine CTRs each year, a mandate to reduce those filings was indeed welcome. Despite industry support for the concept, the number of CTR filings did not drop as dramatically as both the industry and the government had hoped. In fact, in 2002, there were approximately 12 million CTRs, and in 2003 a slight increase. What can be done to bring sanity to a reporting system that includes millions of unnecessary filings?

A February analysis by FinCEN shows that over half of the CTRs filed would be eliminated if the current $10,000 threshold were raised to $20,000 for businesses. The current dollar limit was created close to 35 years ago. [4] While $10,000 is still a large amount of cash for individuals and probably should not be raised, the reports on routine businesses simply clog the system.

Those who would argue that a change in CTR reports will lessen the bank's focus on cash transactions need to be reminded that the industry will still have a reporting infrastructure in place, be required to file SARs on suspicious cash transactions, and would retain the mandate to report individual CTRs over $10,000.

Madam Chairwoman now is the time to adjust a process that is need of repair.

Conclusion

Madam Chairwoman and members of the subcommittee, the ABA has been in the forefront of the industry efforts to develop a strong public-private partnership in the areas of money laundering and

---

[2] See, "The Bank Secrecy Act: Do Reporting Requirements Really Assist the Government?" 44 Alabama Law Review 801 (Spring 1993).

[3] Congress enacted the Money Laundering Suppression Act of 1994 (PL 103-325), which, among other things, mandated that the Treasury Department reduce "routine filings" of currency transactions and establish a central location for the filing of "Suspicious Activity Reports" (SARs) to eliminate duplicative filings.

[4] Several bank economists determined that a proper level for the reporting threshold in 1992 would be close to $36,000. See, Alabama Law Review p. 823. Also see, Conference Report accompanying H.R. 3474 (H. Rept. 103-652) p. 186 (August 2, 1994). ABA found that a CTR could cost an institution anywhere from $3 to $15 to file.

now terrorist financing. This partnership has achieved much success but we know that more can be accomplished. We commend the Treasury Department, banking agencies and FinCEN for their recent efforts to ensure a workable and efficient process. The American Bankers Association will continue our support for these efforts.

Thank you and I would be happy to answer any questions.

TESTIMONY
BY

JOSEPH CACHEY III
VICE PRESIDENT – GLOBAL COMPLIANCE
AND
DEPUTY CHIEF COMPLIANCE OFFICER AND COUNSEL

WESTERN UNION FINANCIAL SERVICES, INC.

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS OF
THE COMMITTEE ON FINANCIAL SERVICES

HEARING ON

"IMPROVING FINANCIAL OVERSIGHT: A PRIVATE SECTOR VIEW OF ANTI-MONEY LAUNDERING EFFORTS"

MAY 18, 2004

GOOD MORNING. I'D LIKE TO THANK YOU ON BEHALF OF WESTERN UNION FOR THE OPPORTUNITY TO ADDRESS THE COMMITTEE ON THE IMPORTANT TOPIC OF THE USA PATRIOT ACT AMENDMENTS TO THE BANK SECRECY ACT AND ITS EFFECT ON MONEY SERVICES BUSINESSES.

WESTERN UNION IS A LEADER IN WORLDWIDE MONEY TRANSFER DOING BUSINESS IN 195 COUNTRIES THROUGH OVER 185,000 AGENT LOCATIONS. OUTSIDE THE UNITED STATES, THE VAST MAJORITY OF OUR AGENTS ARE BANKS OR POSTAL SERVICE SYSTEMS. THESE ENTITIES ARE VERY FAMILIAR WITH DOING BUSINESS UNDER A REGULATORY FRAMEWORK. IN THE UNITED STATES, OUR SERVICES ARE OFFERED THROUGH RETAIL BUSINESSES LIKE GROCERY STORE CHAINS, LOCAL CONVENIENCE STORES AND CHECK CASHERS.

UNDER THE PATRIOT ACT AND THE IMPLEMENTING REGULATIONS, BOTH WESTERN UNION AND ITS DOMESTIC AGENTS REPRESENTING 45,000 INDEPENDENTLY OWNED LOCATIONS HAVE A SEPARATE AND INDEPENDENT OBLIGATION TO IMPLEMENT AND MAINTAIN AN ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM. WESTERN UNION TAKES THIS RESPONSIBILITY SERIOUSLY, AS DO OUR AGENTS. OUR COMMITMENT TO ANTI-MONEY LAUNDERING COMPLIANCE IS

EVIDENCED BY BOTH OUR INTERNAL EFFORTS AND THE SUPPORT WE PROVIDE TO OUR AGENTS.

OUR INITIAL CHALLENGE WITH THE PATRIOT ACT WAS THAT THE REQUIREMENT OF HAVING A FORMAL COMPLIANCE PROGRAM WAS NEW FOR MANY OF OUR U.S. AGENTS. WE MET THIS CHALLENGE BY PROVIDING SIGNIFICANT SUPPORT TO OUR AGENTS TO ASSIST IN THEIR FULFILLMENT OF THE PATRIOT ACT REQUIREMENT OF HAVING AN ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM. AS YOU KNOW, SUCH A PROGRAM MUST INCLUDE DESIGNATION OF A COMPLIANCE OFFICER, WRITTEN POLICIES AND PROCEDURES, MONITORING, EMPLOYEE TRAINING AND A PERIODIC INDEPENDENT REVIEW.

THIS WAS THE FIRST TIME SUCH A REQUIREMENT HAD BEEN PLACED ON OUR AGENTS AND, THEREFORE, WE FACED A STEEP EDUCATION CURVE. TO MEET THIS CHALLENGE, WESTERN UNION INITIALLY DISTRIBUTED A "TURN-KEY" COMPLIANCE GUIDE TO THE ENTIRE AGENT BASE. THIS GUIDE EXPLAINED WHAT A COMPLIANCE OFFICER DOES, AND PROVIDED SAMPLE POLICIES AND PROCEDURES, EMPLOYEE TRAINING MATERIALS AND AN INDEPENDENT REVIEW GUIDELINE. OUR GOAL WAS TWO-FOLD, FIRST, EDUCATE THE AGENT AND SECOND, MAKE COMPLIANCE AFFORDABLE. WE DID NOT WANT

EACH AGENT TO HAVE TO HIRE A LAWYER OR CONSULTANT TO UNDERSTAND THE LAW AND CREATE THEIR PROGRAM.

WE CONTINUE TO ENHANCE THESE EFFORTS OVER TIME. WE HAVE OFFERED OUR AGENTS EXTENSIVE TRAINING OPPORTUNITIES AND WORKSHOPS TO ASSIST THEM IN UNDERSTANDING ANTI-MONEY LAUNDERING ISSUES AND HOW TO BUILD A BETTER COMPLIANCE PROGRAM. WE HAVE DEVELOPED ADDITIONAL MATERIALS, IN A VARIETY OF LANGUAGES, TO ASSIST IN THE DRAFTING OF MORE IN-DEPTH POLICIES AND PROCEDURES. WE ALSO OFFER SELECT AGENTS A TOOL THAT ALLOWS THEM TO MONITOR WEEKLY TRANSACTION ACTIVITY FOR SUSPICIOUS ACTIVITY AT THEIR LOCATION AND WE CONTINUE TO EXPAND THE COMPLIANCE TOOLS WE OFFER OUR AGENTS.

SINCE THE REGULATIONS IMPLEMENTING THE PATRIOT ACT TOOK EFFECT IN JULY, 2002, WESTERN UNION HAS SIGNIFICANTLY ENHANCED ITS OWN TRANSACTION MONITORING CAPABILITIES TO BETTER DETECT AND REPORT SUSPICIOUS ACTIVITY AND LARGE CURRENCY TRANSACTIONS TO THE FINANCIAL CRIMES ENFORCEMENT NETWORK (FINCEN). WE HAVE ALSO INCREASED OUR FRONT-END PROCESSES TO PERFORM MORE ROBUST DUE DILIGENCE

ON THOSE PERSONS WHO WANT TO BECOME A WESTERN UNION AGENT OR HAVE ACCESS TO OUR COMMERCIAL SERVICES.

AS YOU CAN SEE, WESTERN UNION IS TOTALLY COMMITTED TO GETTING THIS RIGHT.

THE DEPARTMENT OF THE TREASURY AND FINCEN REALIZED EARLY ON THAT MONEY SERVICES BUSINESSES WERE NOT BANKS, WE DON'T HAVE AN ACCOUNT RELATIONSHIP WITH OUR CUSTOMERS, WE OFTEN PROVIDE SERVICES ON A ONE-TIME BASIS AND WE OFFER OUR SERVICES THROUGH INDEPENDENTLY OWNED OUTLETS, NOT THROUGH BRANCH OFFICES STAFFED BY OUR OWN EMPLOYEES. BY UNDERSTANDING THESE DIFFERENCES, THE REGULATIONS CALL FOR A RISKED-BASED PROGRAM MEANING THAT A ONE-SIZE-FITS-ALL APPROACH IS NEITHER REQUIRED NOR APPROPRIATE. THIS RISK-BASED APPROACH ALLOWS THE INDUSTRY TO ALLOCATE COMPLIANCE RESOURCES WHERE WE BELIEVE THE MONEY LAUNDERING RISK ACTUALLY IS GREATEST.

FOR EXAMPLE, WESTERN UNION USES A RISK-BASED APPROACH IN SUPPORTING ITS AGENTS. WE CATEGORIZE AGENTS AS NATIONAL ACCOUNTS, NETWORKS AND INDEPENDENTS. NATIONAL ACCOUNTS ARE TYPICALLY PUBLICLY TRADED ENTITIES WITH SUBSTANTIAL

INTERNAL LEGAL AND AUDIT DEPARTMENTS AND EFFECTIVE EMPLOYEE TRAINING PROGRAMS. WITH THESE ENTITIES, WE CAN TAKE A TOP-DOWN APPROACH BECAUSE TYPICALLY THE CORPORATE HEADQUARTERS CAN EFFECTIVELY DRIVE PROGRAMS THROUGH THE ORGANIZATION.

NETWORKS HAVE A REGIONAL PRESENCE, GENERALLY GOOD ORGANIZATIONAL CONTROLS BUT TYPICALLY NEED GREATER ASSISTANCE IN CREATING THEIR PROGRAM AND ROLLING IT OUT TO MULTIPLE LOCATIONS.

INDEPENDENTS ARE COMMONLY REFERRED TO AS "MOM AND POPS" AND NEED THE GREATEST AMOUNT OF ASSISTANCE BECAUSE THEY ARE SMALL BUSINESSES, WITH MINIMAL NEED FOR INFRASTRUCTURE AND TYPICALLY DO NOT HAVE READILY AVAILABLE LEGAL ASSISTANCE.

BY NOT TAKING A COOKIE-CUTTER APPROACH - ALLOWING THE MONEY SERVICES BUSINESS TO DETERMINE THE RISK AREAS AND APPLY RESOURCES APPROPRIATELY – EFFICIENCIES ARE CREATED AND IN THIS MANNER ACTUALLY MORE RISK CAN BE ADDRESSED, MORE EFFECTIVELY.

HOWEVER, RISK MAY SHIFT AS MORE INFORMATION CAN BE OBTAINED AND ANALYZED, AND SO MUST OUR FOCUS. FOR THIS APPROACH TO HAVE THE DESIRED EFFECT, THE REGULATOR, IN THIS CASE FINCEN, MUST PROVIDE ONGOING COMMUNICATION TO INDUSTRY ABOUT EMERGING RISKS AND MONEY LAUNDERING PATTERNS SO THAT THE INDUSTRY CAN DIRECT ITS COMPLIANCE EFFORTS TOWARDS THE MOST CRITICAL RISK AREAS. THIS TYPE OF ONGOING COMMUNICATION SHOULD NOT ONLY RESULT IN MORE MEANINGFUL REPORTING OF SUSPICIOUS ACTIVITY TO LAW ENFORCEMENT BUT ALLOW THE INDUSTRY TO REDUCE THE FILING OF NON-USEFUL REPORTS WHICH MAY CREATE "NOISE" AND UNDERMINE THE EFFORTS OF LAW ENFORCEMENT.

ONE PRIMARY EXAMPLE IS THE REPORTING OF SIMPLE STRUCTURING. CURRENTLY, THE SUSPICIOUS ACTIVITY REPORTING THRESHOLD IS AT $2000 AND STRUCTURING MAY OCCUR JUST BELOW THE $3000 RECORDKEEPING REQUIREMENT. WE NEED TO COLLECTIVELY QUESTION WHETHER FINANCIAL INSTITUTIONS REPORTING ACTIVITY AT THIS LEVEL IS HELPFUL TO LAW ENFORCEMENT. WE WOULD ENCOURAGE FINCEN TO ANALYSE ITS SAR DATA ACROSS THE FINANCIAL SERVICES COMMUNITY AND PROVIDE GUIDANCE ON WHAT TYPE AND LEVEL OF ACTIVITY PRESENTS THE BEST INTELLIGENCE TO LAW ENFORCEMENT. IT IS POSSIBLE THAT BY FOCUSING ON HIGHER

LEVELS OF ACTIVITY WE CAN REDUCE THE NUMBER OF NON-USEFUL REPORTS, ASSIST LAW ENFORCEMENT IN MORE RAPIDLY IDENTIFYING MONEY LAUNDERING SCHEMES AND DRIVE OUR COLLECTIVE RESOURCES TO WHERE THE RISK REALLY LIES.

I AM PLEASED TO NOTE THAT FINCEN DIRECTOR WILLIAM FOX HAS STATED THAT HE AGREES WITH A RISK-BASED APPROACH AND HAS COMMITTED TO FACILITATING BETTER COMMUNICATION EFFORTS WITH INDUSTRY INCLUDING ADDRESSING THE NEED FOR A SIMPLER SUSPICIOUS ACTIVITY REPORT ("SAR") FORM FOR MSBs. IT IS OUR OPINION THAT FINCEN, AS THE POLICY MAKER FOR OUR INDUSTRY, IS IN THE BEST POSITION TO PROVIDE THE NECESSARY GUIDANCE ON THESE ISSUES AND WE ENCOURAGE YOU TO GIVE FINCEN THE RESOURCES NECESSARY TO ALLOW IT TO FULFILL THIS PART OF ITS MISSION. A SINGLE GUIDING VOICE IS BECOMING INCREASINGLY IMPORTANT IN LIGHT OF THE FACT THAT MONEY SERVICES BUSINESSES ARE LICENSED BY THE STATES. WESTERN UNION AND THE AGENT LOCATIONS WE SUPPORT REALLY HAVE 49 REGULATORS: 47 STATES, FINCEN AND THE INTERNAL REVENUE SERVICE (IRS). THIS FRAMEWORK CAN MAKE REGULATORY CONSISTENCY A CHALLENGE.

CERTAINLY AN ISSUE THAT SHOULD BE LOOKED AT IS THE CURRENT BIFURCATION OF THE POLICYMAKING FUNCTION PLACED WITH

FINCEN AND THE TREASURY DEPARTMENT AND THE EXAMINATION FUNCTION LOCATED IN THE IRS. WE ENCOURAGE THE IRS TO ALSO TAKE A RISK-BASED APPROACH IN EXAMINING THE INDUSTRY. IT MAY BE TIME TO REVIEW HOW WELL THE BIFURCATED APPROACH OF THESE AGENCIES IS WORKING. CURRENTLY, BECAUSE THESE REGULATIONS ARE RELATIVELY NEW TO THE INDUSTRY, WE BELIEVE THE MOST WORTHWHILE EFFORTS ARE THOSE FOCUSED ON EDUCATING INDUSTRY PARTICIPANTS AND PREPARATION OF A RISK-BASED EXAM MODEL IMPLEMENTED BY WELL-TRAINED EXAMINERS WHO ARE KNOWLEDGEABLE ABOUT THE INDUSTRY'S RISK-BASED PRACTICES.

WHILE THE PATRIOT ACT HAS PLACED ADDITIONAL RESPONSIBILITIES ON MONEY SERVICES BUSINESSES, OFTEN THERE ARE CALLS FOR ADDITIONAL REGULATION, PARTICULARLY IN THE AREA OF CONSUMER IDENTIFICATION. IN ADDRESSING THESE ISSUES, PLEASE KEEP IN MIND THAT FORMAL, REGULATED MONEY SERVICES BUSINESSES SUCH AS WESTERN UNION, WHILE NOT MAINTAINING CUSTOMER ACCOUNTS, DO KEEP RECORDS OF TRANSACTIONS BOTH BY THE SENDING AND RECEIVING CONSUMER. WE ALSO REPORT ON ANY IDENTIFIED SUSPICIOUS ACTIVITY. THESE RECORDS ASSIST LAW ENFORCEMENT IN THEIR MONEY LAUNDERING INVESTIGATIONS. OVER- REGULATION MAY HAVE THE UNDESIRED EFFECT OF DRIVING

CONSUMERS TO MORE INFORMAL, UNREGULATED SERVICE PROVIDERS THEREBY POTENTIALLY CAUSING LAW ENFORCEMENT TO LOSE SIGHT OF SUSPICIOUS TRANSACTION ACTIVITY AND CLOUDING THE FINANCIAL TRAIL THEY SEEK TO FOLLOW.

FINALLY, A FEW WORDS ON COMBATING TERRORIST FINANCING. AS A GLOBAL COMPANY WE ARE FULLY COMMITTED TO THIS EFFORT. WE MUST RECOGNIZE THAT TODAY'S TERRORIST SEEKS TO WEAVE HIMSELF INTO THE FABRIC OF OUR SOCIETY THROUGH THE CAMOUFLAGE OF FINANCIAL LEGITIMACY. TERRORIST CELLS HAVE LEGITIMATE GOVERNMENT ISSUED IDENTIFICATION, THEY OPEN BANK ACCOUNTS AND HAVE DEBIT AND CREDIT CARDS. THEIR FINANCIAL NEEDS AND TRANSACTIONS MOREOVER MAY ALSO BE SURPRISINGLY SMALL AND CONSEQUENTLY NOT EASILY DETECTED OR PREVENTED. ALL THESE FACTORS MAKE IT NEARLY IMPOSSIBLE FOR A MONEY SERVICES BUSINESS TO FIND THAT NEEDLE IN THE HAYSTACK WITHOUT BETTER INFORMATION FROM THE GOVERNMENT. IF A NAME IS IDENTIFIED BY THE OFFICE OF FOREIGN ASSETS CONTROL AS A SPECIALLY DESIGNATED PERSON, WE WILL STOP THAT TRANSACTION. BUT, I ASK, HOW CAN WE WORK BETTER TOGETHER TO IDENTIFY AND REPORT ON TRANSACTIONS BEFORE THE NAME GETS ON A PUBLICLY AVAILABLE LIST?

IN CONCLUSION, THE USA PATRIOT ACT HAS STRENGTHENED OUR COUNTRY'S ANTI-MONEY LAUNDERING EFFORT SIGNIFICANTLY AND OUR INDUSTRY HAS BEEN THERE EVERY STEP OF THE WAY. BUT TO MOVE TO THE NEXT LEVEL, TO BECOME MORE SOPHISTICATED IN DETECTING AND REPORTING MEANINGFUL SUSPICIOUS ACTIVITY, GOVERNMENT MUST DO A BETTER JOB IN PROACTIVELY COMMUNICATING WITH US. THANK YOU. I WILL BE HAPPY TO ADDRESS ANY QUESTIONS YOU MAY HAVE.

Testimony of Steven Emerson
Executive Director, The Investigative Project
Before the House Financial Services Committee
Subcommittee on Oversight and Investigations
May 18, 2004

The Investigative Project
5505 Connecticut Ave., NW, #341
Washington, DC 20015
Phone 202-363-8602
Fax 202-966-5191
Email: Stopterror@aol.com

Introduction

Madame Chairwoman, Ranking Member Gutierrez, Chairman Oxley, Ranking Member Frank, and all Members of the Committee, thank you for inviting me to participate in this hearing. I commend you on assembling the best panel of private-sector experts on money laundering issues that I have seen at a Congressional hearing in the past two years. They are some of the most influential, knowledgeable, and dedicated experts in the United States and, indeed, the world. I want to thank Jon Levin and Dana Lesemann of The Investigative Project for their work in preparing this testimony.

We are here today to examine whether the Riggs case represents the exception to the rule or the tip of the iceberg. Riggs Bank's failure to file Suspicious Activity Reports (or "SARs") in deference to its clients' desire for secrecy is the single most serious breach ever in the first line of U.S. financial controls against terrorism, and the bank officials who participated in these willful violations should be held personally responsible. SARs are integral to identifying and interdicting illegal assets in the United States. I urge this Committee to conduct a thorough review of the examinations conducted by financial regulators of Riggs and other major financial institutions to see what the regulators knew or should have known of gaps in anti-money-laundering systems.

In at least one instance that I can discuss, a major financial institution cut ties with a terrorist-linked bank upon being advised to do so. In 2000 and 2001, Citigroup was participating in joint ventures with al-Aqsa Bank, which has ties to Hamas. When informed by the Israeli government of those ties, Citigroup contacted the United States Treasury for guidance and subsequently terminated its relationship with al-Aqsa Bank. The question is this: What is the true paradigm? Is it Citigroup's taking the initiative with the Treasury Department or is it Riggs Bank's failure to comply with government mandates? The answer to this question will be critical to determining how you formulate effective measures to interdict terrorism-related transactions in the future.

For those companies that do defy U.S. regulations or fail to prevent their employees from doing so, the recent $100 million fine against Switzerland's UBS AG is a crystal-clear illustration that any short-term profits produced by defying U.S. law will ultimately be overwhelmed by the repercussions of being caught. UBS likely avoided even greater censure by demonstrating that its violations were not part of a greater disregard for financial controls but were isolated actions taken by employees acting contrary to company policy.

However, al-Qaeda has established its own banking system outside of European and U.S. law. Al-Taqwa Bank was created by the Muslim Brotherhood in 1988 to move and safeguard large quantities of cash for terrorist causes; it was finally designated a terrorist entity by U.S. authorities in 2001.

Al-Qaeda and other terrorist organizations have also found innumerable cracks in the financial structures of western nations and exploit the lack of regulation in third-world countries to obscure the sources and destinations of their funds. How has the private sector responded to the revelation that al-Taqwa was a terrorist front? Were private-sector institutions aware of al-Taqwa's links to terror and did they turn a blind eye before the government's designation? Did al-Taqwa's business partners cooperate with U.S. and European investigators once they were made aware of al-Taqwa's links to terrorism? These questions will require your attention and oversight; the answers will guide your approach to regulation of this industry.

As far as maintaining oversight over domestic transactions, the U.S. must continue a multi-pronged approach to countering terrorist money trafficking in the formal international financial

structure. First, programs like the filing of SAR reports and the distribution of information requests under Section 314(a) of the PATRIOT Act must be enhanced, and penalties for non-reporting and non-compliance must be heavy. Second, when terrorists attempt to infiltrate that structure by establishing separate financial institutions, the U.S. must identify them, freeze their assets, and interdict their activities. Last, permanent renewal of a strong and effective PATRIOT Act is fundamental to maintaining maximum pressure on the terrorism's advanced financial apparatus and machinations.

I will now go into more detail about these topics.

Suspicious Activity Reports and Private-Sector Initiation

The SAR report creates an avenue for the U.S. Government to obtain investigative leads from the private sector under reasonable and controlled circumstances. As Comptroller of the Currency John D. Hawke, Jr. said in announcing last week's record fine against Riggs Bank, "[t]he Bank Secrecy Act has been enormously helpful in providing law enforcement agencies with information about illicit activities....Today, it is one more weapon we can to bear in the war on terrorism. The OCC expects banks to have effective anti-money laundering programs in place and we will take strong action against any national bank that is not in compliance with this important law."

Essentially, the SAR rules delineate a set of activities that the government construes to be typical of criminal enterprises and therefore must be reported. This allows law enforcement to generally disengage from the process of examining individual accounts and transactions, and ultimately provides consumers with greater anonymity and an escape from governmental prying. This is the ideal, and, if working effectively, the SAR is a powerful tool through which private sector entities are able to present new investigative leads to law enforcement. There are several weaknesses, however, which might cause the SAR approach to fail.

The Riggs Bank case exhibited one of them; the SAR system is dependant upon profit-driven Banks to take actions that might not be beneficial to their bottom line. According to FinCEN's "Assessment of Civil Money Penalty," May 13, 2004:

> Riggs willfully violated the suspicious activity and currency transaction reporting requirements of the BSA and its implementing regulations, and that Riggs has willfully violated the anti-money laundering program ("AML program") requirement of the BSA and its implementing regulations. The violations Riggs engaged in were systemic – Riggs was deficient in designing a program tailored to the risks of its business that would ensure appropriate reporting, implementing the procedures it did have, and responding to classic "red flags" of suspicious conduct. Riggs failed to correct the violations and implement an adequate BSA program in a timely manner.

Riggs Bank failed to file required SAR reports in deference to its business model. Riggs caters specifically to the diplomatic community, which highly values secrecy. Apparently, those at Riggs who decided that it was best not to file SARs either thought that the business lost would be greater then the cost of non-compliance or that no one would discover their deception. Either way, Riggs employees made a decision to abstain from fulfilling required financial control mechanisms for purely business reasons.

Riggs' program contained serious deficiencies and was not in compliance with the BSA regulations. In January 2003, Riggs' program was deficient in all four elements required by the AML program regulation. Some of the internal control and audit deficiencies continued after the OCC's Consent Order was issued. There are other questions to be answered regarding the Riggs case itself: Were Riggs's clients assured of a quid-pro-quo? How long and with how many clients has Riggs agreed to ignore suspicious activity? To what activities have funds drawn from diplomatic accounts at Riggs gone? Indeed, the most important question to come out of the Riggs case in general is, why did it take so long for this debacle to come to light?

The punitive measures taken by the OCC and FinCEN against Riggs seem appropriate. The $25 million dollar fine levied against Riggs sends a clear message. More important, ultimately, will be the OCC's requirement that Riggs review senior-level competency, develop procedures for ensuring compliance with the Bank Secrecy Act in the future and its examination of past records for irregularities, occasional review of managers' backgrounds, and internal systems for early detection of reporting failures. These specific requirements are a positive step in creating a template for banks rewriting their reporting procedures.

Nonetheless, I urge Congress to conduct a review of the examinations conducted of Riggs by financial regulators both before and after September 11. Riggs's customers and shareholders -- and the public in general -- need to know if regulators missed key indicators that should have warned them of Riggs's noncompliance. There is plenty of precedent for such a Congressional review: in May 2002, this subcommittee conducted a review of SEC examinations of the activities of a crooked stockbroker, Frank Gruttadauria, in connection with your hearing on his theft of millions of dollars from unsuspecting clients. I recall that you found that the SEC missed a key indicator that Gruttadauria may have been illegally churning his clients' accounts. I recommend something analogous to that review. I also hope that you will design a broader review of regulators' examinations of financial institutions, perhaps to be conducted by the GAO with the Inspectors General of the regulators. In this way, the Committee can learn what measures should be considered when debate on the reauthorization of the PATRIOT Act begins next year.

The SAR system itself has only recently caught up to the changing nature of financial crimes and the new focus on their links to terrorism. SAR reports require filers to "characterize" the type of transaction being reported. The list of possible descriptions on the Suspicious Activity Report form includes numerous types of fraud, checking schemes, and identity theft.[1] According to a government publication analyzing the rate and type of SAR filings, "Terrorist Financing was added as a suspicious activity characterization in July 2003; between July and December, 495 SARs were filed with this characterization box marked."[2] It is reasonable to expect that the number of SARs characterized as "Terrorism Financing" will increase substantially in the coming months and years. I know that the Treasury Department's Inspector General is currently conducting a thorough review of the quality of the SAR database and will issue a report in the coming months.

The more difficult task will be to identify ways to make the failure to file SARs a business liability in the future, rather than allowing the Riggs situation to repeat itself. Has the government examined potential changes to the system that will protect financial institutions from the possible economic repercussions of filing SARs? An associated question is whether Riggs was confronted by a specific client or group of clients demanding that Riggs not file SARs. Would such a demand carry its own penalties against the client? Installing protections for financial services against

[1] "The SAR Activity Review; By the Numbers," Issue 2, May, 2004.
[2] "The SAR Activity Review; By the Numbers," Issue 2, May, 2004.

client demands to non-file and the threat of clients withdrawing business will remove an incentive for non-compliance.

Ultimately, the SAR system and automation of information sharing must function successfully for the private sector to be a significant source of counter-terrorism information. A critical improvement in this process would come about by full implementation of the PATRIOT Act Communication System (PACS), which was mandated by Section 362 of the PATRIOT Act to enable financial institutions to file SARs online. Madame Chairwoman, I know that last year you asked the Treasury Department's Inspector General to review PACS implementation, and I hope that that report is available to you and the public soon. PACS has the potential to significantly reduce the costs and improve the efficiency of U.S. anti-money-laundering programs. Timely enactment of the system is vital, though, to provide a sufficient window for evaluating the system prior to reauthorization of the PATRIOT Act.

On a related note, I am aware that testimony before the Financial Services Committee on May 12 suggested that the floor for Currency Transaction Reports (CTR) be raised from $10,000 to $20,000. I urge the Committee to consider that this change would greatly ease transfers of illicit funds by slashing launderers' need to employ complex and stacked transactions and reducing the absolute number of records available to regulators investigating financial crimes.

One final note concerning Riggs Bank; Riggs's transgressions first occurred before the September 11th attacks, and both public and private awareness of the importance of identifying and tracing financial support for terrorism have since changed fundamentally. The implication in the OCC Assessment of Civil Money Penalty that Riggs continued to ignore money-laundering reporting rules, not only after the 9/11 attacks but also after a Consent Order just last year, is devastating. The financial community must understand that their cooperation is fundamental to the war on terror. Riggs's posturing that it was immune to reporting standards because of its clientele is abhorrent, and the officials who committed these egregious violations should be held personally responsible.

Public-Sector Initiation and Public-Private Dialogue

Riggs Bank's failure to comply with money laundering regulations is hardly the sole available example to examine regarding private-public counter-terrorism cooperation. On the contrary, while Riggs may be the worst possible scenario – an institution not only knowingly involved in some manner with financial maneuverings related to international espionage but also explicitly and premeditatedly violating written laws to hide those transactions – other instances in recent years have been effective models of public-private coordination. Citibank's handling of allegations against its corporate partner, al-Aqsa Bank, is an excellent example, the details of which I can discuss now, in contrast to other on-going investigations.

In 1997 $30 million vanished from a Hamas-controlled bank account in Europe.[3] In response, and to protect its remaining and future assets, Hamas established al-Aqsa Islamic Bank that year.[4] Hamas was also operating through another bank, Beit al-Ma'al, for many of its transactions, and al-Aqsa Bank was not used as a conduit until 1999,[5] after Israeli authorities closed down Beit al-

[3] "Hamas Denies Reported Loss of Funds," BBC, October 27, 1997.
[4] Bodansky, Yossef, "Iran's Pincer Movement Gives it a Strong Say in the Gulf and Red Sea," Defense & Foreign Affairs' Strategic Policy, March, 1992.
[5] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.

Ma'al.[6] Al-Aqsa then became a means of circumventing Israeli prohibitions on the activities of Beit al-Ma'al, and a means of evading banking regulations in general.[7] Beit al-Ma'al invested $4,000,000 in al-Aqsa Bank.[8]

After Israel banned al-Aqsa/Beit al-Ma'al's operations,[9] Hamas again bypassed Israeli restrictions and made its funds accessible to Hamas operatives in Israel and the territories by embarking on joint projects with Citibank, intertwining itself with Citibank's Israel division.[10] As part of that relationship, monies deposited into al-Aqsa accounts in Europe or the Middle-East became accessible from Israel through Citibank.[11]

Israeli counterterrorism officials met with Citibank executives in January 2001[12] when Citibank sought to expand its operation in Israel.[13] A Citigroup executive then sent a letter requesting guidance from the U.S. Treasury to Richard Newcomb, Director of the Office of Foreign Assets Control (OFAC),[14] saying "Let me be clear: Citibank would never knowingly do business with a terrorist organization."[15] Neither the Treasury nor Citigroup has released any further correspondence. Citigroup no longer has any relationship with al-Aqsa Bank and noted that, as of January 2001, al-Aqsa Bank was not on the U.S. Government's list of designated terrorist organizations.[16]

Beit al-Ma'al and al-Aqsa Bank were both designated as Global Terrorist entities by the U.S. government on December 04, 2001.[17] The Department of Treasury characterized the designation as "another significant step in the financial war against terrorism."[18]

The al-Aqsa Bank/Citibank episode contains several valuable lessons. First, proper handling by a bank of allegations of wrongdoing is an asset to national security agencies tasked with interdicting terrorist transactions. The manner of federal regulations also leaves banks in a strong position to demonstrate to its clients that it provided information to government only in accordance with legal requirements and is not improperly exposing protected activities or

---

[6] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[7] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[8] Al-Ayyam. July 28, 1999 AND Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[9] "Court Asks State Why it Took $1 Million of HAMAS Cash," Ha'aretz, September 15, 2000.
[10] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[11] Crudele, John, "Citibank Followed the Money Straight to Terrorists," New York Post, February 19, 2002.
[12] Zacharia, Janine, "Citibank Seeks US Guidance Over Hamas Funding," The Jerusalem Post, January 24, 2001.
[13] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[14] Zacharia, Janine, "Citibank Seeks US Guidance Over Hamas Funding," The Jerusalem Post, January 24, 2001.
[15] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[16] Miller, Judith and Atlas, Riva D., "Citibank Weighs Ending Ties With an Arab Bank," The New York Times, January 24, 2001.
[17] Executive Order No. 13224, September 23, 2001, 31 CFR Part 595-597, in Annex dated December 4, 2001.
[18] http://www.treas.gov/press/releases/po841.htm, accessed May 10, 2004.

compromising privacy. Citibank was made aware of a potential problem, gathered information from pertinent government offices, made a determination that its partnership was a liability, and ended the relationship.

Second, it is critical that financial institutions of all types institute systems to prevent flows of funds for terrorist purposes, especially by verifying the identity of customers. "Customer identification programs," or CIPs, are required under Section 326 of the PATRIOT Act. However, customer identification was already becoming a major cost of the operations of a number of major banks before September 11, as many major financial institutions hired senior-level federal anti-money-laundering officials to start "financial intelligence units," or FIUs, even prior to 9/11. Regulatory DataCorp, SAS, and Teledata Communications, among others, are selling special software packages to enable financial institutions to verify customers in real time. I understand that the new AML team at Riggs had not, at least as of this January, adopted an off-the-shelf system. My distinguished colleague on this panel, Jim Richards, has produced invaluable research on the challenges of identifying customers.

The imperfections of the Citibank case, though, are obvious: during the Citibank/al-Aqsa Bank loophole's brief opening Hamas may have moved as much as $1 million into Israel.[19] Moreover, the burden for discovering the loophole in the first place fell entirely upon government agencies that did not have access to banking records that would undoubtedly have facilitated a more rapid investigation. Had the Israeli government not already known that al-Aqsa Bank was an arm of an illegal organization, the Citibank investigation may never have been undertaken.

In contrast, the SAR system creates an opportunity for dialogue initiated by financial institutions. SARs provide the government with indications of financial activity that appear to be typical or indicative of a criminal endeavor, regardless of whether the government is already investigating any of the parties involved in the transaction. Thus, the SARs enable the government to obtain information that might lead to entirely new avenues of investigation. The model SAR-induced investigation would incorporate the process of dialogue we saw in the Citibank case, but would be triggered by the bank's own reporting process.

To improve private-public dialogue, the Department of Homeland Security's Bureau of Immigrations and Customs Enforcement (ICE) has created Operation Cornerstone specifically to liaise with financial institutions. ICE has trained more than 100 Special Agents and deployed them in each of ICE's 27 field offices. This initiative should be monitored and assessed for the extent of the private sector's participation and the coordination among ICE and the FBI, IRS, and other interested agencies.

In addition, Section 314(a) of the PATRIOT Act requires FinCEN to send law enforcement information requests to thousands of financial institutions, which then search their records and transactions, and report positive matches back to FinCEN. FinCEN consolidates the data and provides the information to the law enforcement requestor for appropriate follow-up. Creation of the Section 314(a) system was painful, as John Byrne of the ABA has testified to in the past, but FinCEN's chief of staff reported last week that "law enforcement has discovered over 1,000 items of new financial information resulting in over 500 subpoenas, and other legal process to obtain the documentation for these matches."[20] Most importantly, 314(a) actions have apparently led to

[19] "Top of the News," United Press International, January 25, 2001.

[20] Statement of Robert W. Werner, Chief of Staff, Financial Crimes Enforcement Network, United States Department of the Treasury, before the House Committee on Government Reform, Subcommittee on Criminal Justice, Drug Policy, and Human Resources, May 11, 2004.

arrests and indictments. I recommend that the Committee review the performance of the 314(a) system prior to debate on reauthorization of Title III of the PATRIOT Act.

UBS AG Case

The announcement on Tuesday, May 11 that the U.S. Government will levy a $100 million fine against the Swiss bank UBS AG for engaging in currency transactions with states subject to U.S. sanctions sends a very strong message and sets a positive precedent. According to media reports, UBS's contract with the United States Treasury stipulated that UBS not trade with nations subject to U.S. sanctions,[21] but that UBS nonetheless traded with Libya, Iran, Cuba, and Yugoslavia.[22]

According to initial reports, the UBS violations were committed by a group of individuals in contravention of company policy.[23] The Federal Reserve said in a statement that, "[i]n violation of law, certain former officers and employees of UBS engaged in intentional acts aimed at concealing those bank- note transactions from the reserve bank, including, but not limited to the falsification of monthly reports submitted by UBS to the reserve bank."[24] UBS reportedly terminated employees who aided the illegal transactions.[25] UBS said in a statement that it "has already instituted corrective and disciplinary measures and has decided to exit the international banknote trading business."[26] UBS and the U.S. government have approached the punishment and prevention of this crime appropriately. UBS identified the cause of the problem and instituted policies to prevent a recurrence. The U.S. government levied a heavy penalty that fairly reflected the severity of the crime.

However, as with the al-Aqsa and Riggs cases, the impact of the breach in financial controls is irreversible. U.S. policy, embodied in Section 311 of the PATRIOT Act, is to deny certain countries the benefits of economic interaction with the United States as punishment for severe state crimes, and such sanctions are a cornerstone of U.S. interaction with hostile nations. We should not hesitate to employ the most severe sanctions against countries that fail to cooperate with us in fighting terrorism.

Terrorist Entities' Methods of Financing: Bank al-Taqwa

Unfortunately, as illustrated tangentially by the al-Aqsa Bank/Beit al-Ma'al investigation, today's sophisticated terrorist organizations do not rely upon conventional financial services companies, but have created a wholly independent set of institutions. It is safe to assume that terrorist financiers and companies will not fulfill SAR reporting requirements or cooperate with government investigations.

---

[21] Paletta, Damian, "UBS Fined $100 Million on Currency Violations," The American Banker, May 11, 2004.
[22] Paletta, Damian, "UBS Fined $100 Million on Currency Violations," The American Banker, May 11, 2004.
[23] Paletta, Damian, "UBS Fined $100 Million on Currency Violations," The American Banker, May 11, 2004.
[24] "Swiss Bank UBS Pays 100-Million-Dollar Fine for Abusing Fed Account," Agence France Presse, May 10, 2004.
[25] "Feds Fine UBS $100 Million For Illegal Cash Transfers," Wall Street Journal Online, May 10, 2004.
[26] "Feds Fine UBS $100 Million For Illegal Cash Transfers," Wall Street Journal Online, May 10, 2004.

According to President Bush, Bank al-Taqwa is "an association of offshore banks and financial management firms that have helped al-Qaeda shift money around the world."[27] Al-Taqwa was founded as the first step in "establishing a world bank for fundamentalists" and to compete with Western financial institutions.[28] Al-Taqwa's connections to al-Qaeda led the Bush administration to freeze al-Taqwa's assets on November 7, 2001.[29]

In January, 2002, the Treasury Deputy General Counsel wrote to Swiss official M. Claude Nacati that, "Bank al-Taqwa...was established in 1988 with significant backing from the Egyptian Muslim Brotherhood, and it has long been thought to be involved in financing radical groups like the Palestinian HAMAS, Algeria's Islamic Salvation Front, and Armed Islamic Group, and Tunisia's An-Nahda."[30] The Deputy General Counsel also wrote that, "[a]s of October, 2000 Bank Al Taqwa appeared to be providing a clandestine line of credit for a close associate of Usama bin Laden."[31] Al-Taqwa reportedly has offices and activities from Panama to Kuwait.[32]

Unlike al-Aqsa Bank or Beit al-Ma'al, al-Taqwa Bank was able to function entirely on its own, without relying on the patronage of a larger organization. By avoiding interaction with the legal financial community, terrorist organizations evade government regulations such as SAR reports entirely. Indeed, although it is not yet clear whether Riggs Bank made a simple business decision that not filings SARs would be beneficial to its standing among its target clientele or in fact instituted procedures to defy federal regulations, al-Taqwa and other terrorist institutions exist specifically to design means of circumventing government controls.

Al-Qaeda and other terrorist organizations have diversified means of obtaining cash, both legally and illegally, which must be passed from its multitude of sources to many fewer end-users without identifying the earners, the means of passage, or the receivers. All of the produce of terrorist schemes involving counterfeit baby formula, CDs, and DVDs, schemes to profit on un-taxed cigarettes and other products, credit card fraud, smuggling, and a slew of other petty crimes must be laundered. While hawalas and suitcases full of cash have served to pass significant quantities of cash, al-Qaeda's financial apparatus is integral to the smooth operation of al-Qaeda's network of members and affiliates.

Indeed, Osama bin Laden came to prominence among the Afghan Mujahideen precisely because of his talent for moving men and money around the world without governmental interference. Every government victory in interdicting terrorist finances today is being examined by our enemies for lessons-learned, which are then incorporated into the organizations and companies replacing those we have shut down.

---

[27] "President Announces Crackdown on Terrorist Financial Network," November 7, 2001, http://www.state.gov/s/ct/rls/rm/2001/5982.htm.

[28] Bodansky, Yossef, "Iran's Pincer Movement Gives it a Strong Say in the Gulf and Red Sea," Defense & Foreign Affairs' Strategic Policy, March, 1992.

[29] Executive Order No. 13224, September 23, 2001, 31 CFR Part 595-597, in Annex dated November 7, 2001.

[30] Letter from George B. Wolfe, Deputy General Counsel of the U.S. Department of the Treasury, to M. Claude Nicati, Substitut du Procureur General, Switzerland, January 4, 2002.

[31] Letter from George B. Wolfe, Deputy General Counsel of the U.S. Department of the Treasury, to M. Claude Nicati, Substitut du Procureur General, Switzerland, January 4, 2002.

[32] "Money Laundering Probe to Look at Possible Bin Laden Link," Agence France Presse, September 23, 2001, and Executive Order No. 13224, September 23, 2001, 31 CFR Part 595-597, in Annex dated November 7, 2001. Various sources have referenced al-Taqwa activity in Liechtenstein, Italy, Malta, Panama, Switzerland, France, Kuwait, the United Arab Emirates, and the Bahamas...

Conclusion

If in fact Riggs's failure to file SARs was merely an oversight or profitable omission, then it is an issue that can and will be addressed neatly and thoroughly. The UBS precedent is a good one, and should guide responses to similar financial crimes in the future. Clearly, corporate structures that aid or abet defiance of federal regulations knowingly must be met with stiffer penalties. However, the vast majority of both passive and active institutional violation of governmental controls is going to be the result of profitability, not a desire to aid terrorists.

Although the Riggs case represents the failure of the financial sector in oversight, there are cases and examples that represent the courageous successes of financial institutions of monitoring suspicious activities and actually helping the government to track and interdict possible terrorist operations. . In this category is a fellow panelist, Jim Richards, who has played a singular role in helping the government identify terrorists in the United States because of his dedication and tireless commitment to the security of this country.

On the other hand, constituents of a small subset of financial institutions that violate government proscriptions are constituted for the express purpose of providing services to terrorists. The long-term challenge posed by al-Taqwa and similar terrorist-controlled institutions is that their schemes might easily elude detection for many years. From the highest corporate structures such as al-Taqwa to the petty crimes such as fraud, counterfeiting, theft, and smuggling, al-Qaeda and other terrorist organizations have diversified means of raising and moving financial assets.

Vigilance by private industry sources in filing SARs and similar accounting documents are vital to exposing not only terrorist transactions passing through their own institutions but also institutions that are themselves fundamentally terrorist in nature.

STEVEN EMERSON
EXECUTIVE DIRECTOR
THE INVESTIGATIVE PROJECT

Steven Emerson is an internationally recognized expert on terrorism and national security, a correspondent, and an author who also serves as the Executive Director of The Investigative Project, the nation's largest archival data and intelligence on Islamic and Middle Eastern terrorist groups. He is most recently the author of the national best seller, "American Jihad: The Terrorists Living Among Us" (Free Press). Mr. Emerson is widely recognized as one of the foremost experts in the world on militant Islamic terrorism. Since September 11, 2001, Mr. Emerson has appeared frequently on network television and has been quoted or cited hundreds of times in the nation's top newspapers. Mr. Emerson and his institute have also given numerous briefings to Congress, the White House, the Justice Department and other federal agencies.

Mr. Emerson started The Investigative Project in late 1995, following the broadcast of his documentary film, "Jihad in America," on Public Television. The film exposed video of clandestine operations of militant Islamic terrorist groups on American soil. For the film, Mr. Emerson received numerous awards including the George Polk Award for best television documentary, one of the most prestigious awards in journalism. He also received the top prize from the Investigative Reporters and Editors Organization (IRE) for best investigative report in both print and television for the documentary. The award from the IRE was the fourth such award he had received from that group. The documentary, which was excerpted on *60 Minutes*, is now standard viewing for federal law enforcement and intelligence organizations.

Over the past three years, Mr. Emerson has testified more than two dozen times before Congress, and he has briefed the National Security Council at the White House as well.

Mr. Emerson has authored or co-authored five books:

"American Jihad: The Terrorists Living Among Us" (Free Press, 2002)
"Terrorist: The Inside Story of the Highest-Ranking Iraqi Terrorist Ever to Defect to the West" (Villard/Random House, 1991)
"The Fall of Pan Am 103: Inside the Lockerbie Investigation" (Putnam, 1990)
"Secret Warriors: Inside the Covert Military Operations of the Reagan Era" (Putnam, 1988)
"The American House of Saud: The Secret Petrodollar Connection" (Franklin Watts, 1985).

"Steve Emerson deserves the highest prize - a Pulitzer or whatever it may be - for investigative journalism." U.S. Representative Christopher Smith (R-NJ)

Richard Clarke, former head of NSC Counterterrorism, in a feature article on Emerson in Brown Alumni Magazine (November-December 2002), said, "'I think of Steve as the Paul Revere of terrorism... [Clarke] credits Emerson with repeatedly warning of Al Qaeda sleeper cells in the United States. He adds that he would attend Emerson's speeches whenever possible because 'we'd always learn things we weren't hearing from the FBI or CIA, things which almost always proved to be true.'"

Andrew McCarthy, Assistant U.S. Attorney who prosecuted the 1993 World Trade Center bombings, said in the same feature article on Emerson in Brown Alumni Magazine (November-December 2002) "...Emerson was helpful in preparing to cross-examine defense witnesses in the [1993 World Trade Center bombings] case....He's a valuable source of information and knowledge. And in terms of trying to find places to look for evidence, he's a very good person to talk to. He's got a lot of insight."

Robert Blitzer, former Chief of the FBI's Domestic Terrorism/Counter-Terrorism Planning Section, has said, "Steve Emerson has tremendous information and I have no doubt that he is better informed in many areas of terrorism than we were in the government."

Testimony of

James R. Richards

On Behalf of

BANK OF AMERICA

Before the

House Financial Services Subcommittee on Oversight and Investigations

On

Improving Financial Oversight: A Private Sector View of Anti-Money Laundering Efforts

May 18, 2004

Thank you, Madam Chairman and members of the Subcommittee for the opportunity to testify today on the private sector's views of the current anti-money laundering efforts and the oversight of those efforts.

My name is Jim Richards. I am a Senior Vice-President and the Global Anti-Money Laundering Operations Executive, Compliance Risk Management, for Bank of America. Prior to the merger of Bank of America and FleetBoston Financial, I was the Director of Fleet's Financial Intelligence Unit, or FIU. In both roles, I have or had responsibility for the bank's operational aspects of preventing, detecting, and reporting potential money laundering or terrorist financing.

I have been asked to testify today about whether and how the current regulatory regime under the Bank Secrecy Act and USA PATRIOT Act can be fine-tuned to better achieve institutional integrity and national security goals, and what recommendations I may have to make compliance with those laws more effective.

Let me first emphasize that my comments here today reflect the views and experiences of Bank of America and the anti-money laundering group that I have had the pleasure of being a part of over the last five years at the former FleetBoston Financial. For the most part, these views coincide with those of our private sector and public sector partners.

Also, in addressing these issues, the view, or perspective, I bring to this Subcommittee is that of someone who sees the Bank Secrecy Act and USA PATRIOT Act, regulations, and regulatory guidance first hand and in operation. My experience and perspective is that of someone operating a unit within a financial institution that is responsible for investigating and reporting suspicious activity to the Government, and how the changes since the tragic events of September 11th and the passage of the USA PATRIOT Act have impacted that function. In order to illustrate some of the hands-on functions, I will briefly describe some of the technology, tools, and techniques we have used in those

efforts. I thank you for the opportunity to share these views and this testimony with the Committee.

From a purely operational point of view, or from the perspective of implementing the BSA and USA PATRIOT Act, money laundering is not terrorist financing and terrorist financing is not money laundering: they are two very different problems that need to be addressed very differently. That said, from our financial institution's perspective, the issues of money laundering and terrorist financing both require that financial institutions creatively review and match internal and external data and information relating to transactions and relationships.

Finally, detecting terrorist financing or terrorist financing-related transactions is virtually impossible. We rely almost exclusively on the Government to provide us with information we then use to attempt to identify potential terrorist financing activity or individuals or entities involved in terrorist financing.

I. From a Financial Institution's Perspective, There Are Fundamental Differences Between Money Laundering and Terrorism Financing

Although there are hundreds of different types of crimes, for the purposes of money laundering prevention in the financial services industry, there are only two types of crimes: crimes for profit, such as narcotics trafficking or securities fraud; and crimes of purpose, such as terrorism.

These two classifications of crimes are very different, and pose incredible differences in how they are detected and, hopefully prevented, in the financial services sector. Understanding these differences is the key to building an effective anti-money laundering (AML) and terrorist financing prevention (TFP), detection, mitigation, and remediation program that addresses all of the relevant compliance risks, regulatory risks, reputational risks, and legal risks.

Traditional crimes for profit have been the focus of our money laundering laws since the passage of the Bank Secrecy Act in 1970. The "profit" aspect of these crimes allowed legislators, regulators, law enforcement, and the private sectors to focus on transactions – high volume, large dollar, high velocity transactions detected internally, then reported to the Government either through a Currency Transaction Report, or CTR (for cash transactions greater than $10,000) or a Suspicious Activity Report, or SAR (for all transactions greater than $5,000 that fit the definition of "suspicious").

Beginning with the recordkeeping and cash reporting requirements of the Bank Secrecy Act in 1970, moving to the money laundering crimes of the Money Laundering Control Act of 1986, and to the suspicious transaction reporting requirements of the Money Laundering Suppression Act of 1992, the focus of financial institutions was inward or internal - on the transactions being conducted to, from, or through the institution. Monitoring systems were built for cash transactions and wires; surveillance tools were developed to allow institutions to look at what defined classes or groups of customers were doing; and many banks began to develop ad hoc or specialized databases and processes to allow for more proactive analysis, investigation, and reporting of suspicious activity.

Since the tragic events of September 11th, we have learned that terrorist financing is very different than traditional money laundering.[1] September 11th and the passage of the USA PATRIOT Act (the "Patriot Act") forty-five days later changed the focus from internally-sourced cases originating from reviews of high-velocity, high-dollar transactions to externally-sourced cases originating from requests from law enforcement through the provisions of OFAC, section 314(a) of the Patriot Act, or grand jury subpoenas. The

[1] I draw a distinction between the schemes used to fund a particular terrorist cell or terrorist operation, such as the funding of the various September 11th hijacker cells, from the greater financing of terrorist organizations, such as the use of narcotics trafficking and kidnapping to finance Colombia's FARC and ELN, or the abuse or misuse of charitable organizations. There is a distinction between the methods used to fund a particular cell or operation and those used to support the long-term financing of an organization.

Patriot Act also added, for the first time, a requirement that all financial institutions have a program to verify the identity of their new customers.[2]

So now financial institutions have two very different issues before them: how to identify and report suspicious activity sourced from internal monitoring and surveillance of transactions; and how to identify and report the existence of customer relationships sourced from external requests for information. Put another way, money laundering prevention is a transaction-focused, internally-sourced issue, where transactions lead to relational links; terrorist financing prevention is a relationship-focused, externally-sourced issue where relational links lead to transactions.

Exhibit A shows two "screen shots" – one of a typical pre-9/11 money laundering investigation, showing entities linked by clustered transactions; and one of a typical post-9/11 terrorist financing investigation, showing the often random and cluttered relational links between entities, addresses, corporate or business relationships, and other commonalities.

Three scenarios are also illustrative of the differences between internally-sourced transactional money laundering investigations and externally-sourced relational terrorist financing reviews:

> Scenario 1 - A branch manager notices that a customer has come in twice a day every Friday for three weeks, depositing between $6,000 and $8,000 in small denomination bills each time. These "structured" transactions make no sense for this particular customer.
>
> Scenario 2 - A transaction monitoring system looks at all customers that

[2] Section 326 of the Patriot Act requires all financial institutions to have reasonable, risk-based procedures for verifying the identity of any person seeking to open an account, to the extent reasonable and practicable. Obtaining basic identifying information on customers, being ably to verify that information, and being able to compare this information with the customer's actual activity is the heart and soul of any effective anti-money laundering program.

open accounts without a Taxpayer Identification Number, with opening deposits of less than $1,000, with structured cash deposits and ATM withdrawals in high-risk countries. These customers may be involved in traditional money laundering.

Scenario 3 - A customer opens up a checking account and obtains an ATM/debit card. He has a random but normal number of small cash and check deposits, and has a number of small ATM cash withdrawals. He purchases one money order for less than $1,000, which is eventually cashed in a known high-risk terrorism country.

The first two scenarios may be examples of money laundering. At the very least, they are easily detected by rudimentary "money laundering" transaction-focused monitoring and surveillance tools and techniques. The third scenario is absolutely benign and virtually impossible to detect as either money laundering (which it isn't) or terrorist financing ... unless the government provides the institution with the name of the customer through the section 314(a) process. With the name and perhaps address and any other identifying information, financial institutions can then begin to form relational connections (common telephone numbers, common addresses, linked accounts, etc.): with those relationships come transactions with other customers or other entities. Ultimately, when put together, a potential pattern of possible terrorist financing may emerge.

In a traditional money laundering case, banks identify potentially unusual transactions through electronic or human means, then conduct a review of those transactions in attempt to answer the question "do these transactions have a business or apparent lawful purpose or are they the sort in which the particular customer would normally be expected to engage, and is there a reasonable explanation for these transactions after examining the available facts, including the background and possible purpose of them?"[3] If the answer to this (complicated and lengthy) question is "no", then the bank has an obligation to file

[3] Paraphrasing the language found in the SAR regulation at 31 CFR 103.18(a).

a Suspicious Activity Report (SAR). The financial services industry has spent the last thirty years developing programs, systems, databases, and training for this money laundering problem. The regulatory community has well-established examination guidelines that give the industry a road map on how to meet its obligations. Organizations such as the American Bankers Association offer guidance and assist the industry in developing "best practices". But what about the new obligations imposed by the Patriot Act? These new obligations have forced us to take a new look at relationships and transactions, internal and external data and information, and how we put these together.

II. The Data and Information Available to Financial Institutions

Just over five years ago I was asked to build a comprehensive anti-money laundering group and function at BankBoston.[4] At the time, BankBoston had a BSA compliance program, including the required recordkeeping and reporting functions. What we built was a group that complemented those existing resources, but was focused on proactive prevention, detection, and mitigation of all risks relating to money laundering: compliance, regulatory, reputational, operational, and legal risks. We began, literally, with 2 people and 2 laptops: by the end of 2003 we were 24 people running an in-house-built Money Laundering Deterrence database that cost something less than $250,000 for the computer hardware, and we were running what we then called our Financial Intelligence Unit, or FIU, for one of the ten largest banks in the country. Currently, as part of the new Bank of America, we are in the process of taking the best practices from both organizations and integrating them into a new, combined group within Compliance Risk Management reporting to the Bank's Chief Compliance Executive, Charles Bowman. Working very closely with me and also reporting to Mr. Bowman is Daniel D. Soto, one of the most respected professionals in this field. Where my focus is on AML operations, Dan is responsible for AML and OFAC policies and procedures as the Global AML and OFAC Program Executive. It is an excellent partnership.

[4] In October, 1999 BankBoston and Fleet Bank merged to form FleetBoston Financial. In April, 2004 FleetBoston Financial was purchased by Bank of America.

Whether preventing, detecting, or investigating the movement of funds generated by or used for traditional crimes or terrorism, a financial institution must focus on answering a central question:

> Do we know, suspect, or have reason to suspect that a transaction or series of transactions "has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and [we] know[] of no reasonable explanation after examining the available facts, including the background and possible purpose of the transaction"? *Quoting 31 CFR 103.18(a)*

Breaking down this requirement gives us the factors we need to consider and data or information we need to access. Essentially, we have Customers, with Products, doing Transactions, through Delivery Channels, at Locations, in Certain Amounts. These factors, when broken down into their most basic components and matched with what you know – both from internal "know your customer" or "enhanced due diligence" as well as external, publicly-available information – are the cornerstones of any effective program. Exhibit "B" shows these factors, with some detail, and they are explained in some detail below.

- Customers – prior to the passage of the Patriot Act, most banks had developed "Know Your Customer" programs. Section 326 of the Patriot Act and accompanying regulations have imposed a risk-based regime for verifying the identity of new customers and for existing customers opening up new accounts in certain circumstances. But for the purposes of building an effective AML (anti-money laundering) system, it can be argued that there are really only a few different types of customers: existing customers vs. new customers; customers with an identified relationship manager vs. customers without; and U.S. customers (or persons) vs. non-U.S. customers (or persons).[5] Also, whether a

[5] The difference between U.S. persons and non-U.S. persons is codified at 31 CFR 103.121(a)(3). The tools and information available to verify the identity of a U.S. Person are better than the tools and information available to identify non-U.S. persons seeking to open an account.

customer is a primary account signer, or the principal of a corporation, trust, or other legal entity may determine what information is available.

- Products – the principle transactional products in most banks are checking accounts (demand deposit accounts, or DDAs) and savings accounts.

- Transactions – all transactions that can be conducted at or through a financial institution are relevant for the purposes of detecting and/or preventing money laundering and terrorist financing. All transactions fall into one of three buckets - cash, electronic, or paper – and are either credits (incoming) or debits (outgoing). All transactions in whatever form and moving in whichever direction are eventually captured electronically in one or multiple bank systems. The key is to be able to find those electronic records and access them. Given the volumes of transactions in many large institutions, this can be a daunting if not close to impossible task. However, certain transactions are more likely to be used than others. These would include large cash and structured cash transactions, wire transfers, and large checks. Other potentially high-risk transactions include the purchase or redemption of bank checks or travelers checks and ACH transactions.

- Delivery Channels – Transactions are conducted at or through various delivery channels. Traditionally, the branch was the channel through which most retail transactions flowed. With the advent of electronic banking, many customers never transact at a branch, so the human contact is often minimal.[6] Transactions conducted through ATMs will have varying amounts of information, depending on whether they are solely cash transactions, or "mixed" cash and checks; whether they are in-branch ATMs, ATMs owned and serviced by the bank, or

[6] For many banks, their branches are still a principal source of potentially unusual or suspicious transactions. This first-level of defense – a person seeing something unusual and reporting it to a central AML group for further analysis and review – is a critical component of an effective AML monitoring and surveillance program.

ATMs serviced by third-party vendors. Other delivery channels include point-of-sale debit and credit locations, and, most recently, the Internet.[7]

- Locations – the key data or information characteristics of locations are whether the location is inside or outside the United States and whether the location of the transaction is different than the domicile of the customer.

- Amounts – the amounts of the different types of possible transactions is also a critical piece of data or information. Three different scenarios are possible: the transaction or series of transactions are under the recordkeeping thresholds (such as the $3,000 threshold for wire transfers or monetary instruments); whether the transaction or series of transactions are under the reporting thresholds (such as the $10,000 threshold for cash transactions); and whether the transaction or series of transactions are anomalous for the type of customer, product, account, transaction type, delivery channel, or location.

- External Factors – perhaps the most important information available is not internal customer or transaction information, but publicly-available, external information that is available to be used to determine, confirm, or suggest that the transaction or transactions in question make sense. Examples of the sources and uses of this external data are discussed below.

Once a financial institution has identified all of these sources or types of data and information, and found a way to access that data, they must be brought into a centralized data management tool so that the people or group responsible for the AML program can monitor transactions, conduct surveillance of high-risk customers, and perform ad hoc queries. Coupled with a robust case management system and an ability to capture potential new cases identified by bank associates in the branches and elsewhere, this group can then perform the analysis, investigations, reporting, trending, and remediation,

[7] Delivery channels are also critical at the account opening stage of the relationship: the mechanics of opening an account and obtaining and verifying any identification documents will vary depending on the

and help support the front-end and continuing enhanced due diligence needed to protect the institution from the myriad of risks posed by money laundering and terrorist financing.

III. Using Existing Desktop Technology to Prevent and Detect Potential Money Laundering or Terrorist Financing Activity

Since the tragic events of September 11th, dozens if not hundreds of companies have come forward with new money laundering or terrorist financing "solutions." Some of those tools[8] are excellent; others have little or no value. However, the financial services industry, like most people, tends to embrace new technology or tools without fully understanding the new technology and without having fully used or implemented the old or existing technology. Indeed, two of the finest anti-money laundering and terrorist financing prevention tools that are available today are already on most banks' shelves and on most bankers' desktops, and are customizable to any institution, of any size. If used creatively and well, these tools can form the cornerstones of most institutions' AML programs. These two common tools – basic database software such as Microsoft Excel™ and the Internet – can be the most effective tools available.

1. Basic Database Tools & Techniques – Really Using Microsoft Excel™

The Financial Intelligence Unit at the former FleetBoston Financial conceived, built, and operated a Money Laundering Deterrence (MLD) Database that monitored and could query transactions running through roughly 20 million accounts. Both the hardware and software were "off the shelf", and the only "customized" aspects were the reports, queries, and macros that were written by the FIU staff themselves. We looked at vendor "solutions", but kept going back to our own system as we found it was more effective,

account opening channel – whether in person, over the telephone, or through the Internet.

[8] The terms "AML Solution" or "Due Diligence Solution" or "Patriot Act Solution" are invariably used by vendors. The term "solution" in the context of anti-money laundering and terrorist financing prevention is not only misplaced, but misleading: there are *tools* that, used creatively and well, allow financial institutions to better detect, investigate, and report activity and transactions that could be indicative of potential money laundering or terrorist financing. Unfortunately, there are no solutions.

flexible and user-friendly than anything else we saw. But one of the key aspects in developing and running our in-house system was the ability to utilize the tools and attributes inherent in the software. The best example of this is our use of two of the most useful, but least known, features of the most commonly used desktop database software, Microsoft Excel™. These two features, used separately or together, turn this basic program into the most effective AML and TFP tool available today:

(a) Filters

As seen in the five figures of Exhibit C, the "filter" function in Excel™ allows the user to drill down into a category or attribute of data. In the example shown, a database of 10,000 wire transfers is "filtered" so that the user only sees those transactions where the customer name contains the terms "import" and/or "export." Other "filters" could include a specified date range, a dollar threshold or exact dollar amount, or transactions within a specified date range between certain dollar collars (say, between $8,000 and $10,000) conducted only by customers with an address in Boston, Massachusetts where the beneficiary of an outgoing wire or originator of an incoming wire has an account with a US financial institution with an ABA routing number beginning with "1149."[9]

The filter function is particularly effective for parsing the data or information contained in or needed for Suspicious Activity Reports, such as customer and suspect attributes, branch of account and activity, type of activity, description of activity, and whether any law enforcement agency was contacted. With this data and information contained in a simple spreadsheet, the bank could perform sophisticated reporting, trending, and

[9] Identifying banks through their ABA routing numbers or, in the case of international banks, by their SWIFT bank identification codes, is often more effective than identifying them by name. ABA routing numbers are 9 digits: the first two digits represent their Federal Reserve District; the third and fourth digits represent the city or region within that District; the fifth through eighth digits represent the specific bank; and the ninth digit is an algorithmic key to prove the legitimacy of the number. In the illustration given, ABA routing numbers beginning with "1149" are banks in the 11th Federal Reserve District (Texas) generally along the Rio Grande River from El Paso to Brownsville. SWIFT bank identification codes have an eight-figure (alpha-numeric) root where the first four digits represent the bank, the fifth and sixth the two-digit country code, and the seventh and eighth the city or region within the country. CITIUS33, for example, would be Citibank in the United States, in New York.

"lessons learned" in order to focus training and reduce the incidence of laundering in the future. Using the filter function, the BSA Officer could look at SARs filed by state where the activity was described as structuring and the description of the activity included the term "money service business" or "wire transfer". Using simple graphing and mapping features found in Excel™ and companion programs such as MapPoint™, the BSA Officer could easily focus his efforts on particular branches.[10]

(b) Pivot Tables

Most average users of Excel™ have at least a passing understanding of the Filter function. Very few even know that the "Pivot Table" function exists. The Pivot Table function allows the user to summarize data and the relationships between the different types of data elements within a spreadsheet very quickly. It automates what most people now do manually.

For example, in the 10,000-wire table described above, a typical investigation may want to focus on one customer or contra party. More importantly for money laundering, however, is the need to identify patterns, trends, or anomalies within large amounts of data such as this. The ability to manipulate this data is critical.

The three Figures shown in Exhibit "D" give a very simple example of how to construct a Pivot Table. In this case, we are building a table that summarizes all of the transactions between our 125 customers and the various contra parties, by the total amount of the wires between any one customer and any one contra party. We could also look at the total number of transactions between them, the average dollar amount, the range of wires,

[10] This is an example of the concept that, from the perspective of a bank's risk officer, money laundering or terrorist financing is not a problem, but a symptom of an underlying operational or control problem. When looked at from this perspective, the risk officer is able to look at the filing of a SAR or the activity represented in the SAR as a symptom of an underlying problem with account opening procedures, document collection and verification procedures, branch AML training, or the monitoring or surveillance functions. Looking at money laundering or terrorist financing as a symptom rather than a problem can be an effective way to focus on and eliminate or mitigate the underlying causes.

or virtually any other characteristic of the transactional relationship between the two types of entities. A similar exercise could be done if the database included relational data, such as customers and addresses by city, state, or country. Adding some "high risk" transactions, such as "structured" cash transactions or foreign ATM transactions, would allow the user to construct a Pivot Table showing all customers, arranged by state, and the number or dollar amount of their high risk transactions.

2. The Internet – Perhaps The Finest EDD/AML/TFP Tool Available Today

Who are your customers? Who are they transacting with? Is your customer really affiliated with that company in Texas? Is your customer's business really located at that address? Does the telephone number Area Code match the address Zip Code? Is the transaction the sort in which the particular customer would normally be expected to engage?

The answer to these questions often can be found through publicly available, free, searchable databases, search engines and web directories contained on the Web and accessed through the Internet. Although many financial institutions pay vendors for "due diligence" or other services, and many of these data aggregator vendors offer outstanding value and service, many institutions should also take advantage of what is available on the or through the Internet. Over the last five years, the associates in the (former Financial Intelligence Unit of FleetBoston Financial and now) Global AML Operations unit of Bank of America have developed some creative and useful tools and techniques for accessing, exploring, utilizing, and harvesting information from the Internet. In the course of developing and sharing these tools and techniques, it has become apparent that although almost everyone uses these tools, they don't generally use them well, thoroughly, or creatively. Indeed, the biggest barrier to finding and using the vast amount of information available on or through the Internet is the lack of courage or initiative to "click something new every day." Most of the tools and techniques described herein were found by exploring the Web, or by clicking something new or different.

(a) The Surface Web

The search engines and web directories that 99% of people use can be found on what is known as the "surface web." These include such staples as Google™, AllTheWeb™, DogPile™, and Kartoo™. Very simply, surface web search engines have software programs that scour the Web, locating web pages and web page links and pulling those pages back to the search engine's database where they are stored and made accessible by keyword searches. Through Google™, for example a user can access over 3.5 billion web pages, hundreds of thousands of images, millions of old Newsgroup messages, and a 30-day archive of news stories from over 4,500 worldwide sources. A user can also translate a phrase or even translate an entire web site; or search for a key phrase in country-specific sites. Other surface web sites such as VisualRoute™ or BetterWhoIs™ allow the user to track down the physical location of a website's server or obtain the name of the person or entity that owns the domain name. Other specialized sites, such as www.findinformation.homestead.com put hundreds of free, publicly available databases and search tools into one site or location for ease of use.

(b) The Invisible Web

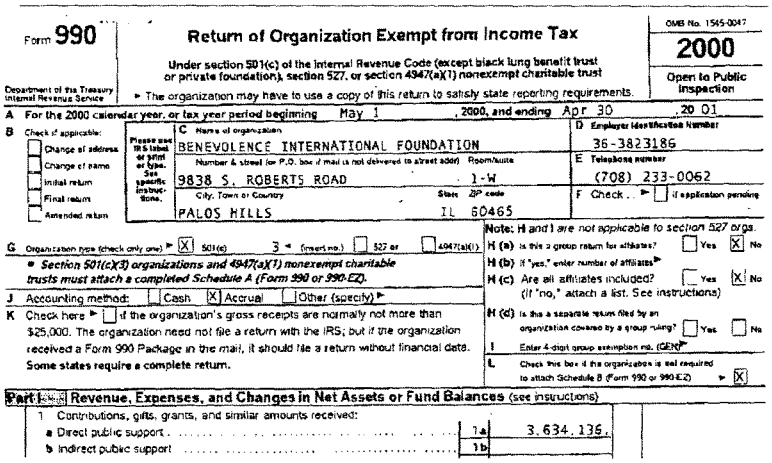
Surface web search engines give their users links to, perhaps, 5 to 10 billion documents that have been posted on the Web. But there are billions of documents and databases that, by their nature or because of the economics or other quirks of search engine technologies, either cannot be located or accessed through those search engines or are not located or accessed. These documents or databases that cannot or are not accessed through the surface web, can be accessed through what is known as the Deep Web or Invisible Web, and number in the hundreds of billions.[11] Public databases, such as state corporate records, may be found by a regular search engine query, but generally can be accessed only through the invisible Web.

[11] One of the best explanations of the invisible web is "The Invisible Web: Uncovering Information Sources Search Engines Can't See," Chris Sherman and Gary Price, Cyber Age Books, Medford, NJ 2003.

One of the best Invisible Web sites, and one of the best enhanced due diligence, anti-money laundering, or terrorist financing prevention tools available today is the databases found at www.searchsystems.net. SearchSystems™ has assembled approximately 19,000 free searchable public records databases from around the world. Focused primarily on Canada and the United States, this site gives the user a remarkable access to public records. Exhibit "E" is a screen shot of the Search Systems™ home page.

An example of a typical terrorist financing review may be that conducted by many banks on an entity known as Benevolence International Foundation, or BIF. BIF had its assets frozen by the US Government in December, 2001 under allegations that it had ties to or was involved in providing material support to a Foreign Terrorist Organization. In late January 2002 BIF filed suit against the US Government, denying ties to terrorism. An affidavit filed in support of that action was signed by a BIF principal, Enaam Arnout. Mr. Arnout eventually admitted in a plea agreement of moving money to Muslim fighters in Bosnia and Chechnya, and in February 2003 he pleaded guilty to one count of conspiracy.

When faced with these facts, many financial institutions reviewed their customer and transactional systems to determine if they had BIF as a customer. Who or what was BIF, and who was affiliated with BIF? One of the first places to go to answer those questions could be SearchSystems™ or another invisible web site such as www.guidestar.org, a database of millions of US-registered charitable organizations. GuideStar would have given you access to the following:



Form 990 — Return of Organization Exempt from Income Tax

Under section 501(c) of the Internal Revenue Code (except black lung benefit trust or private foundation), section 527, or section 4947(a)(1) nonexempt charitable trust

► The organization may have to use a copy of this return to satisfy state reporting requirements.

OMB No. 1545-0047 — 2000 — Open to Public Inspection

Department of the Treasury Internal Revenue Service

A For the 2000 calendar year, or tax year period beginning May 1, 2000, and ending Apr 30, 20 01

B Check if applicable: Change of address; Change of name; Initial return; Final return; Amended return

Please use IRS label or print or type. See specific instructions.

C Name of organization: BENEVOLENCE INTERNATIONAL FOUNDATION

Number & street (or P.O. box if mail is not delivered to street addr): 9838 S. ROBERTS ROAD — Room/suite: 1-W

City, Town or Country: PALOS HILLS — State: IL — ZIP code: 60465

D Employer identification number: 36-3823186

E Telephone number: (708) 233-0062

F Check ► ☐ if application pending

Note: H and I are not applicable to section 527 orgs.

G Organization type (check only one) ► [X] 501(c) 3 ◄ (insert no.) ☐ 527 or ☐ 4947(a)(1)

• Section 501(c)(3) organizations and 4947(a)(1) nonexempt charitable trusts must attach a completed Schedule A (Form 990 or 990-EZ).

H (a) Is this a group return for affiliates? ☐ Yes [X] No

H (b) If "yes," enter number of affiliates ►

H (c) Are all affiliates included? ☐ Yes [X] No (If "no," attach a list. See instructions)

H (d) Is this a separate return filed by an organization covered by a group ruling? ☐ Yes ☐ No

I Enter 4-digit group exemption no. (GEN) ►

J Accounting method: ☐ Cash [X] Accrual ☐ Other (specify) ►

K Check here ► ☐ if the organization's gross receipts are normally not more than $25,000. The organization need not file a return with the IRS; but if the organization received a Form 990 Package in the mail, it should file a return without financial data. Some states require a complete return.

L Check this box if the organization is not required to attach Schedule B (Form 990 or 990-EZ) ► [X]

Part I Revenue, Expenses, and Changes in Net Assets or Fund Balances (See instructions)

1 Contributions, gifts, grants, and similar amounts received:

a Direct public support . . . . . 1a 3,634,136.

b Indirect public support 1b

(c) The Historical Web

Where the Surface Web and Invisible Web allow you to search for and obtain documents or gain access to databases that are currently available on the Web, the so-called "Historical Web" gives you access to much of what was once on the Web but is no longer there. A remarkable site is that of the Internet Archive, available at www.archive.org (see Exhibit "F"). This site, and its "Wayback Machine", gives access to much of what was on the Web, back to 1996. Very simply, the Internet Archive has taken electronic "snapshots" of virtually everything on the Web at various points of time, back to 1996, and stored it on their servers. Most important, these documents are available to everyone.

An interesting example of the investigative utility of the Internet Archive is the website www.azzam.com, "widely considered to be the premier English-language mouthpiece of Al-Qaida."[12] If one were to try to pull up this site today, it would be gone or unavailable,

[12] Testimony of Steven Emerson, Executive Director, The Investigative Project, before the House Committee on Financial Services, Subcommittee on Oversight and Investigations, "Terrorism Financing & U.S. Financial Institutions," March 11, 2003. Hearings on "Progress Since 9/11: The Effectiveness of U.S. Anti-Terrorist Financing Efforts"

having been "pulled" some time after September 11th. However, by simply typing in the URL, or web address, into the WayBack Machine, the investigator can gain access to virtually every rendition of the Azzam site, back to 1999, including almost every document posted on the site (almost 2,100 pages or documents).[13]

IV. Conclusion

The success of our anti-money laundering and terrorist financing prevention efforts is entirely dependent on cooperation between and coordination by all of the parties involved: the law enforcement and intelligence communities, the regulatory community, the private sector, our trade associations, and others. The collaborative efforts of all of these groups in the drafting of regulations implementing the USA PATRIOT Act, particularly for sections 314(a) and 326, has resulted in regulations that are reasonable, effective, and balance the needs of the law enforcement community with the obligations and realities facing the private sector.

From the perspective of an individual financial institution – indeed, the group within that institution that is responsible for operationalizing many of the obligations imposed by the Bank Secrecy Act and USA PATRIOT Act - the simple fact remains that in order to effectively meet these duties and obligations we will continue to depend on cooperation and assistance from our partners and colleagues in the public sector, including the regulatory agencies.

Operationalizing the provisions of the Bank Secrecy Act and USA PATRIOT Act has been and continues to be a complex endeavor. From the policies, procedures, and practices for know your customer or enhanced due diligence; to the systems and tools to monitor transactions and conduct surveillance of high-risk customers or classes of customers; to the ability to analyze, investigate, and report suspicious activity; and to trending, training and testing for and of those programs, the tasks of individual financial

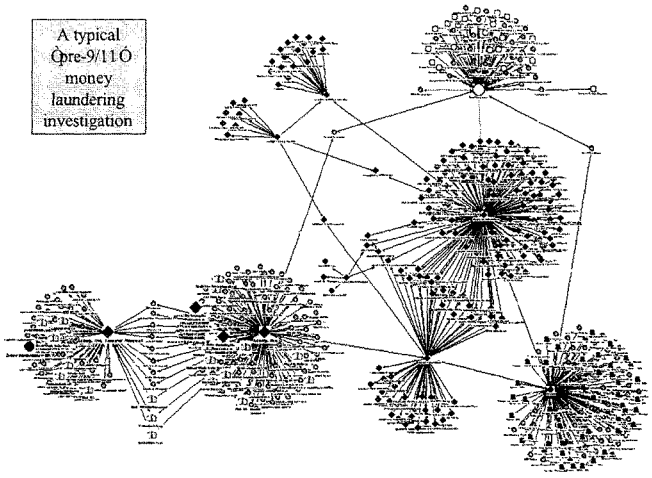
[13] The user will find that not all portions of web sites are included: those portions that are memory intensive, such as flash media or other animations, are generally not captured in the Archive.

institutions are daunting. As daunting is the task of the regulatory community to set standards for and examine those programs. Continued cooperation and dialogue between the regulatory community and the institutions it regulates is critical to understanding and controlling the unique risks posed by money laundering and terrorist financing.

Thank you for this opportunity to testify on this very important topic. Bank of America remains committed to meeting its obligations of detecting, preventing, reporting, and mitigating the effects of money laundering and terrorist financing, and recognizes and applauds the efforts of its private sector colleagues and public sector partners in these efforts.

Exhibit "A"

Data Visualization of a Money Laundering Investigation and a Terrorist Financing Investigation



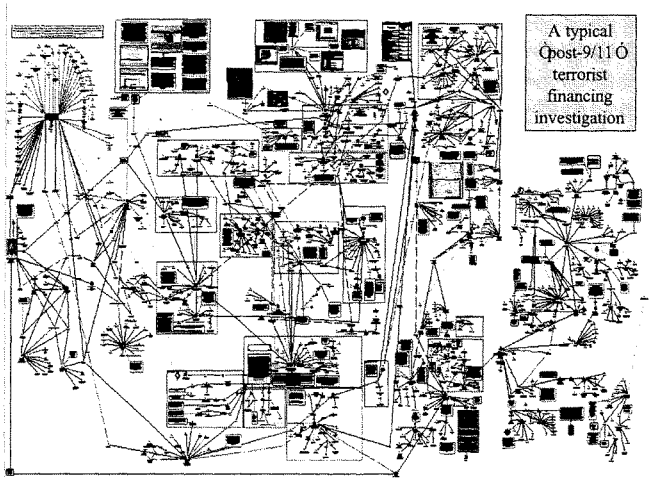
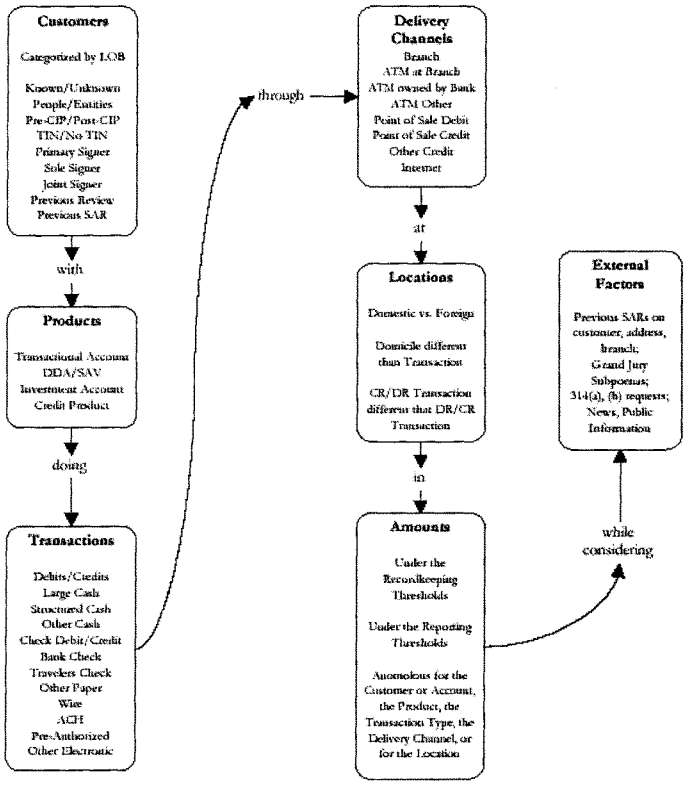


Exhibit "B"

Data and Information Building Blocks



May 18, 2004

Exhibit "C"

The Use of The "Filter" Function in Microsoft Excel™ as an AML and TFP Tool

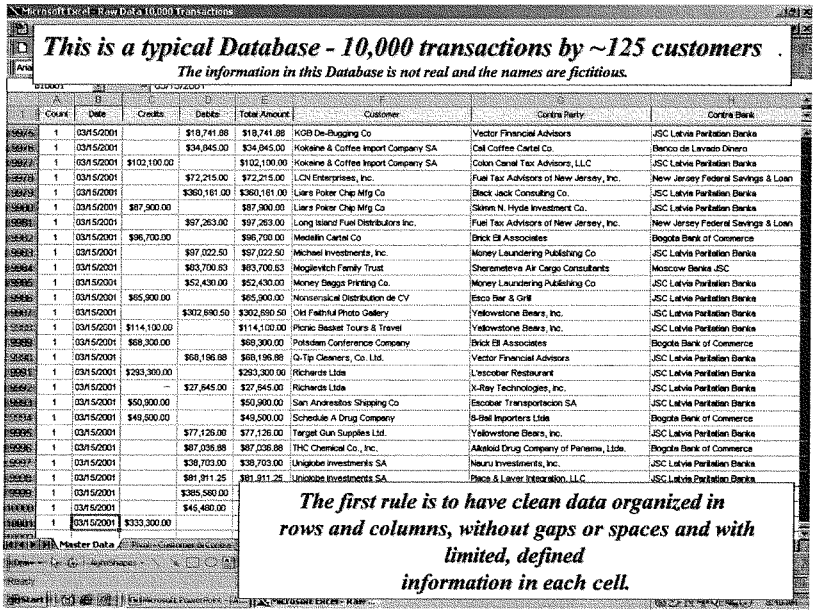


Figure 1 – A "typical" transactional database showing 10,000 transactions. In this example, we created a database of fictitious wire transfers, showing the date, whether the wire was incoming or outgoing, the customer name, the "contra party" name (the originator of an outgoing wire or the beneficiary of an incoming wire), and the contra party's bank. This table shows 10,000 transactions conducted by approximately 125 fictitious customers to approximately 100 fictitious contra parties.

Exhibit "C" (continued ...)

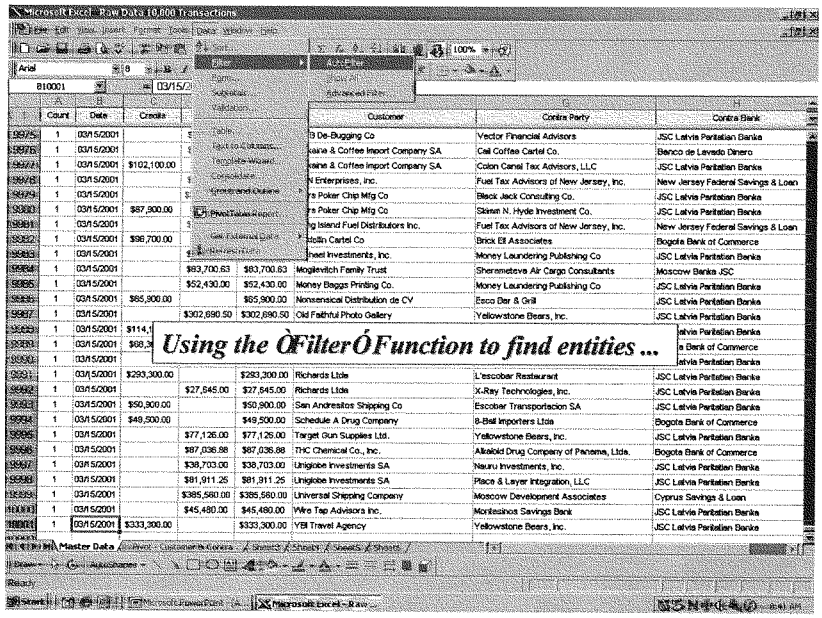


Figure 2 – To turn on the "Filter" function, find and click on the "Data" menu to reveal a drop-down list of commands. Scroll down that list with your cursor to the "Filter" command. Sub-commands will appear on the right: slide the cursor over to "apply" and click. The drop-down menu will disappear, and small arrows or indicators will appear in the bottom-right hand corner of the column headings.

Exhibit "C" (continued ...)

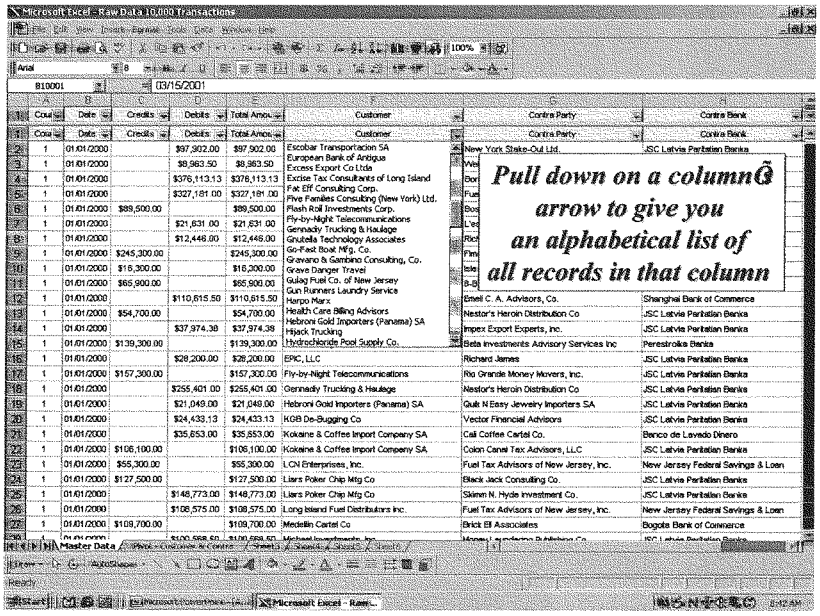


Figure 3 – Small drop-down arrows appear on the column headings. Clicking on any of those arrows allows you to pull down on that column, giving you a numerical or alphabetical list of all records in that column. In this case, we have pulled down the "customer" column, revealing a list of all customers that conducted wire transfers, arranged alphabetically. We could do the same for the Date column, Amount column, or any other column in the database.

Exhibit "C" (continued ...)

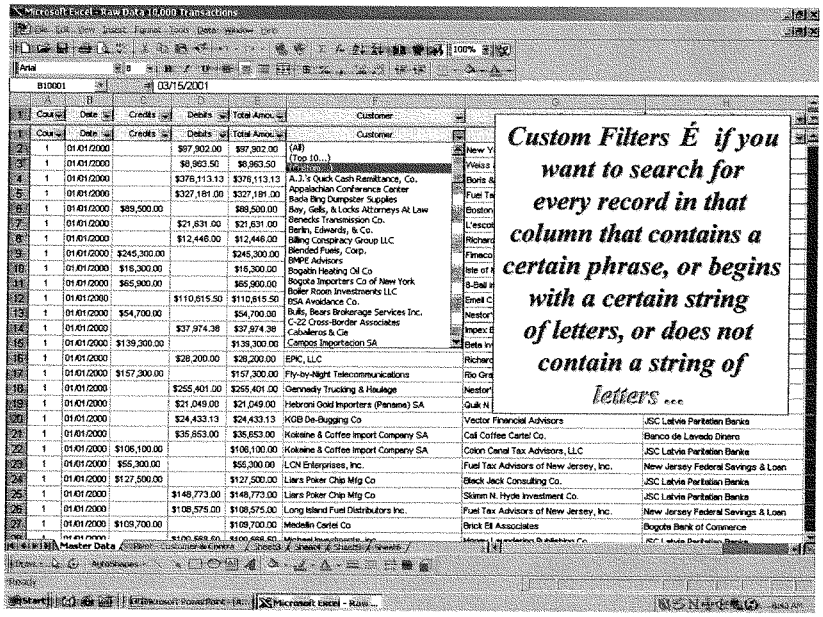


Figure 4 – At the top of the drop-down alpha/numeric list are three other choices: show All, show the Top 10, or "Custom". The Custom feature is incredibly useful, allowing you to search every record in the column for a certain phrase or combination of phrases, a certain string of letters, a particular date range, or any other factor. It also allows you to exclude a phrase, number or date.

Exhibit "C" (continued ...)

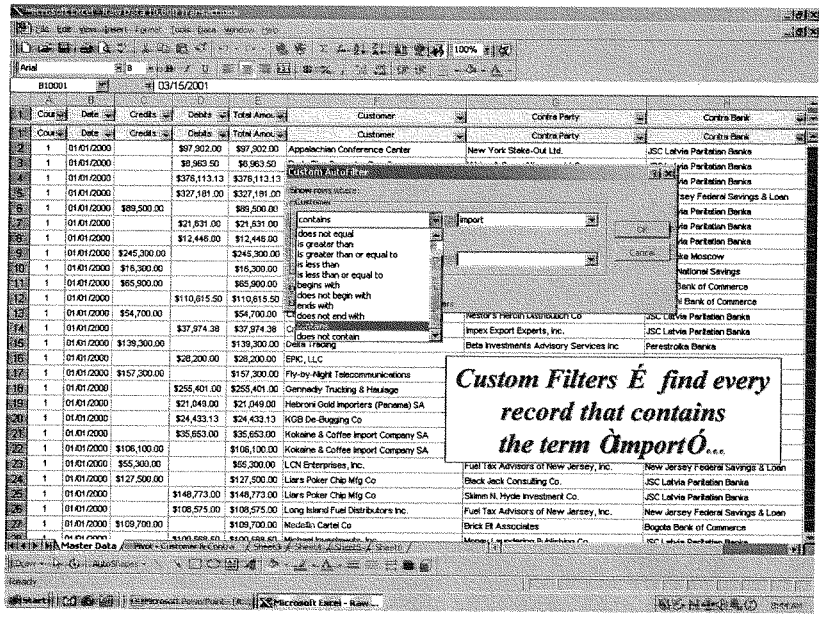


Figure 5 – In this case, we have filtered our "customer" column so that we are going to see only those customers whose name contains the term import. Here, you have two choices: you can include those customers whose name contains "import" AND the term "export", or you could include those customers whose name contains the term "import" BUT NOT the term "export." The possibilities are endless.

May 18, 2004

Exhibit "D"

The Use of The "Pivot Table" Function in Microsoft Excel™ as an AML/TFP Tool

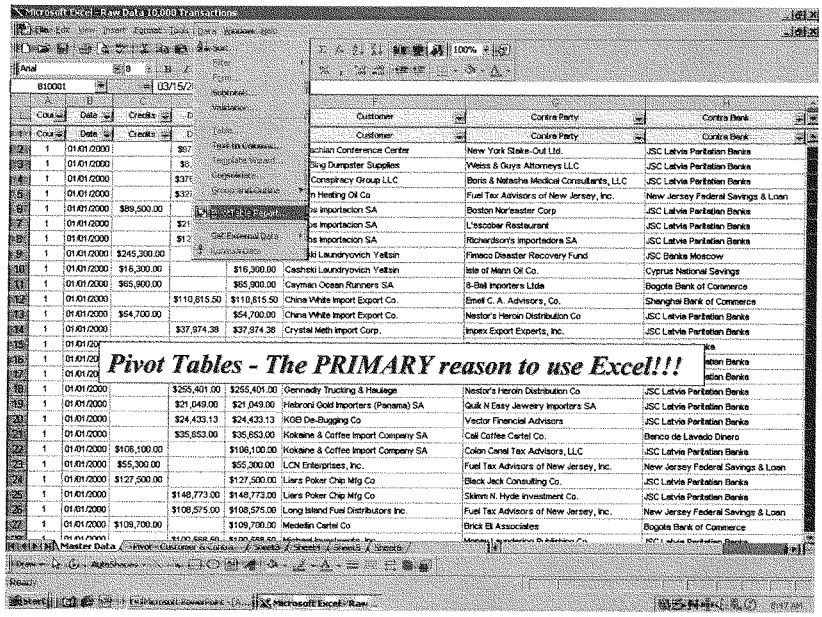


Figure 6 – Like the "Filter" function, the "Pivot Table" function appears in the "Data" drop-down list located at the top of the control panel in Excel™. Clicking on the "Pivot Table" command opens up a "Wizard" that guides you through the steps needed to build the Pivot Table.

Exhibit "D" (continued ...)

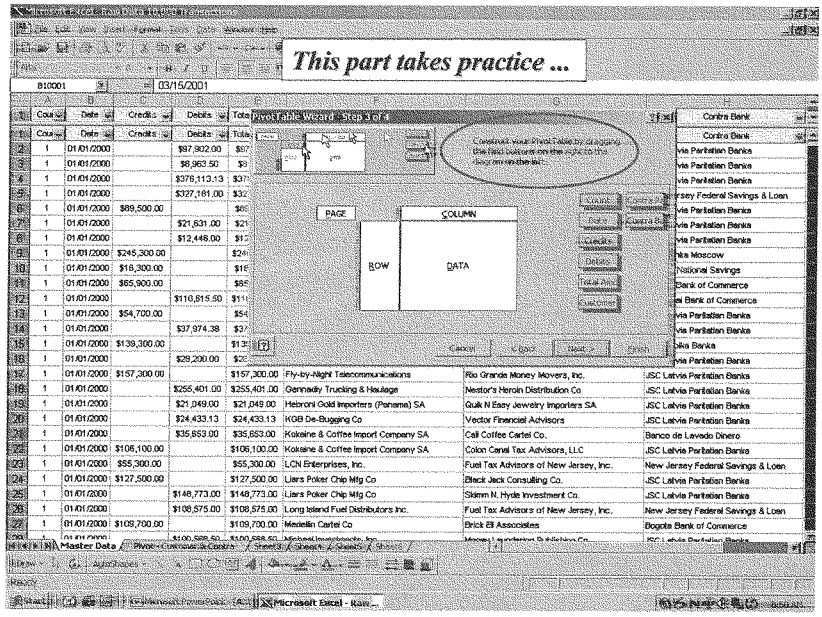


Figure 7 – The "Wizard" walks you through the steps needed to build the Pivot Table. This takes some practice, as you need to learn the best ways to build your table, dragging column headings represented by the buttons on the right of the drop down menu into the table located on the left.

Exhibit "D" (continued ...)

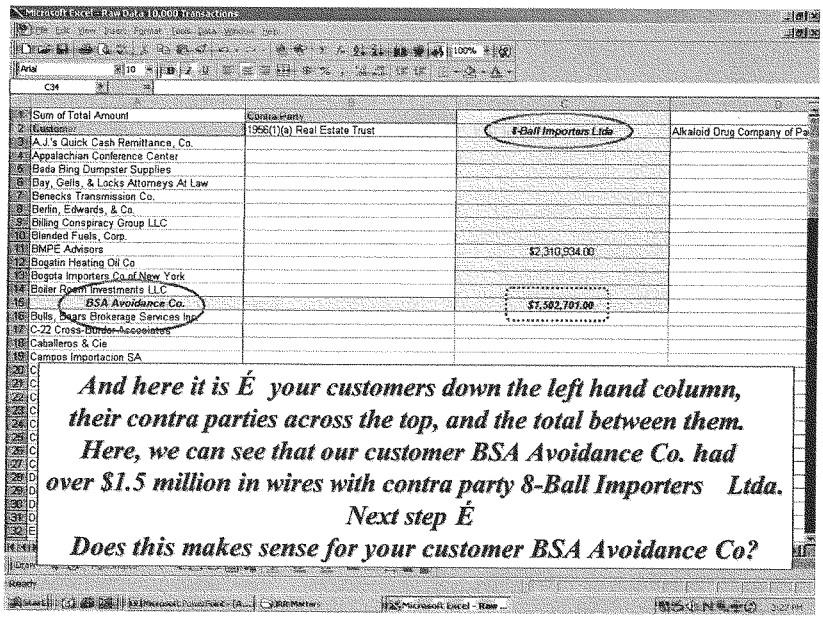


Figure 8 – In this case, we built a Pivot Table from our wire transfer database showing all customers down the "Y" or left hand column, all contra parties across the top (originators of incoming wires or beneficiaries of outgoing wires), and the sum of the wires between any customer and any contra party (in this case, rather than the sum of the wires, you could choose the average wire, largest wire, number of wires, or even the standard deviation between the wire amounts).

Exhibit "E"

The Invisible Web – www.searchsystems.net

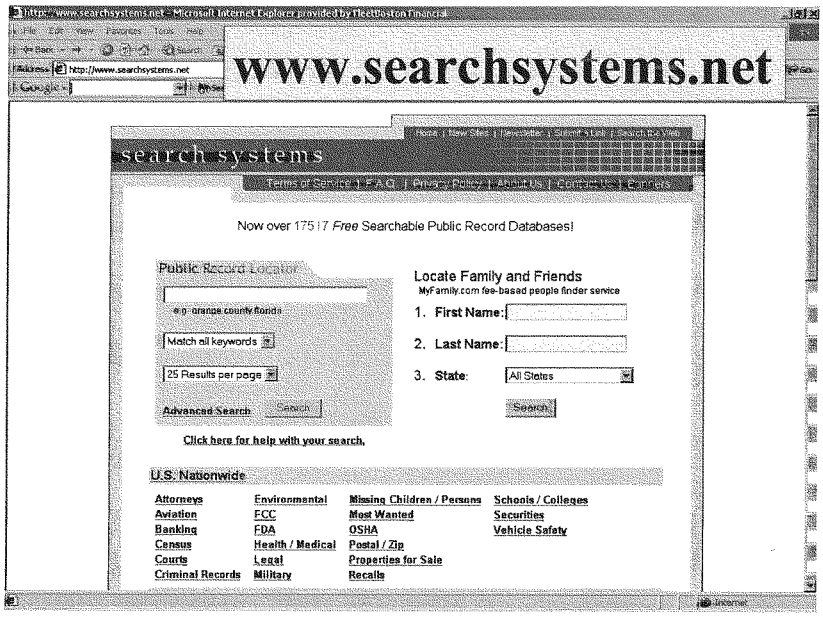


Figure 9 – www.searchsystems.net gives the user free access to thousands of publicly available databases. In the United States, the majority of these are state-by-state.

May 18, 2004

Exhibit "F"

The Internet Archive's Site at www.archive.org and the "WayBack Machine"

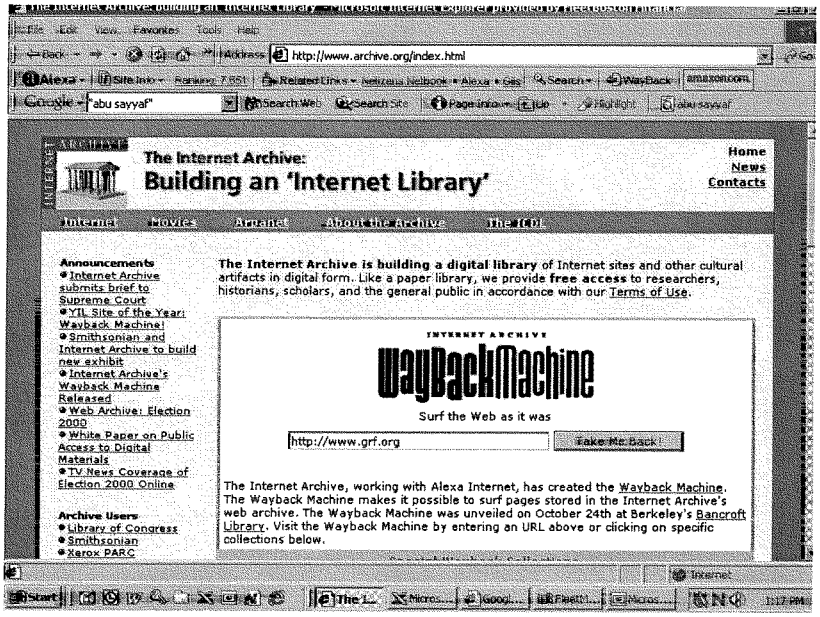


Figure 10

Exhibit "F" (continued ...)

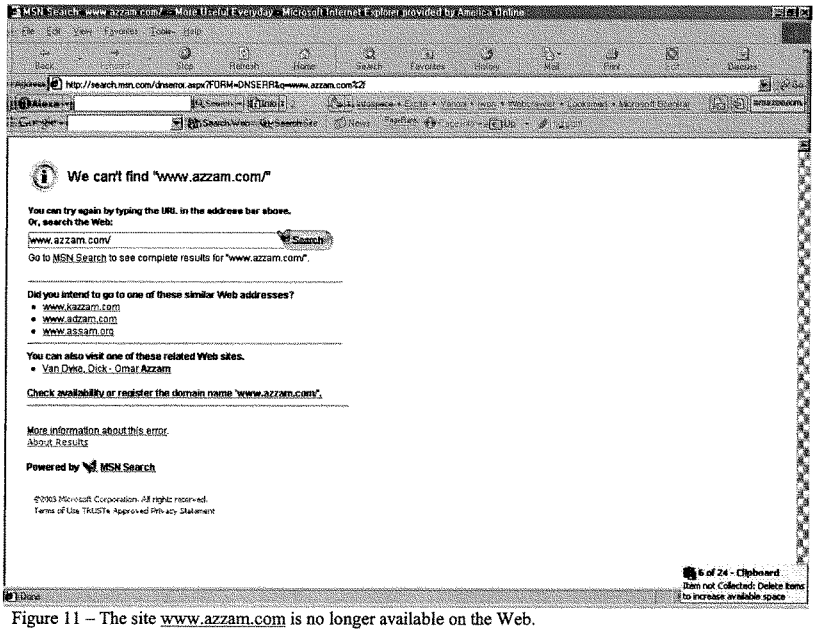


Figure 11 – The site www.azzam.com is no longer available on the Web.

Exhibit "F" (continued ...)

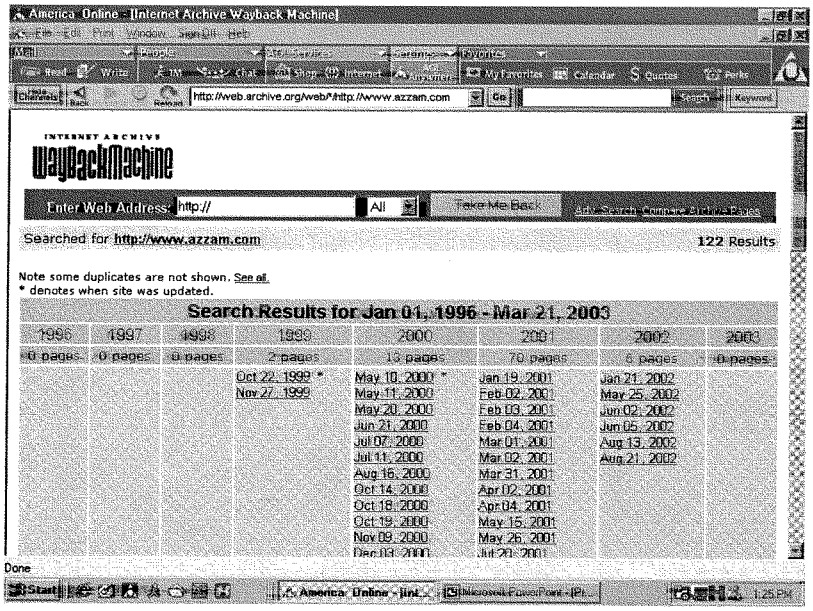


Figure 12 – Entering the URL www.azzam.com into the WayBack Machine lists 91 web pages that Azzam has had back to October 22, 1999. Clicking on one of them will pull back the archived version of that site. Entering the URL followed by "gibberish" will return all pages and documents attached to those 91 web pages. In the case of Azzam, there are almost 2,100 such pages.

May 18, 2004

Exhibit "F" (continued ...)

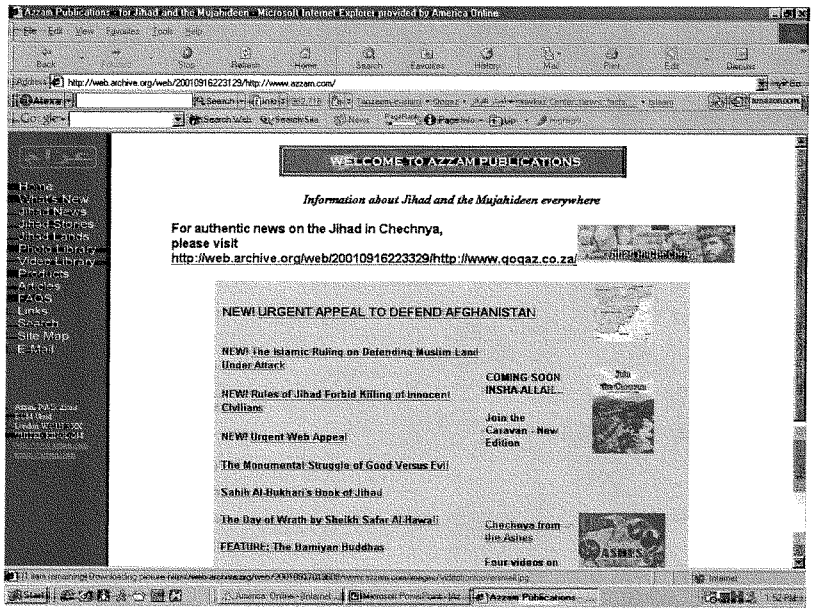


Figure 13 – This is a screenshot of the URL for www.azzam.com from the WayBack Machine's archive dated September 16, 2001. Notice the "New!" section titled "Urgent Appeal to Defend Afghanistan".

o