AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

A REVIEW OF CURRENT AND EVOLVING TRENDS IN TERRORISM FINANCING

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

SEPTEMBER 28, 2010

Printed for the use of the Committee on Financial Services

Serial No. 111–161

U.S. GOVERNMENT PRINTING OFFICE

62–686 PDF WASHINGTON : 2010

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

BARNEY FRANK, Massachusetts, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
MAXINE WATERS, California
CAROLYN B. MALONEY, New York
LUIS V. GUTIERREZ, Illinois
NYDIA M. VELÁZQUEZ, New York
MELVIN L. WATT, North Carolina
GARY L. ACKERMAN, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
DENNIS MOORE, Kansas
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
CAROLYN McCARTHY, New York
JOE BACA, California
STEPHEN F. LYNCH, Massachusetts
BRAD MILLER, North Carolina
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
MELISSA L. BEAN, Illinois
GWEN MOORE, Wisconsin
PAUL W. HODES, New Hampshire
KEITH ELLISON, Minnesota
RON KLEIN, Florida
CHARLES WILSON, Ohio
ED PERLMUTTER, Colorado
JOE DONNELLY, Indiana
BILL FOSTER, Illinois
ANDRÉ CARSON, Indiana
JACKIE SPEIER, California
TRAVIS CHILDERS, Mississippi
WALT MINNICK, Idaho
JOHN ADLER, New Jersey
MARY JO KILROY, Ohio
STEVE DRIEHAUS, Ohio
SUZANNE KOSMAS, Florida
ALAN GRAYSON, Florida
JIM HIMES, Connecticut
GARY PETERS, Michigan
DAN MAFFEI, New York

SPENCER BACHUS, Alabama
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
RON PAUL, Texas
DONALD A. MANZULLO, Illinois
WALTER B. JONES, JR., North Carolina
JUDY BIGGERT, Illinois
GARY G. MILLER, California
SHELLEY MOORE CAPITO, West Virginia
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
J. GRESHAM BARRETT, South Carolina
JIM GERLACH, Pennsylvania
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
PATRICK T. McHENRY, North Carolina
JOHN CAMPBELL, California
ADAM PUTNAM, Florida
MICHELE BACHMANN, Minnesota
KENNY MARCHANT, Texas
THADDEUS G. McCOTTER, Michigan
KEVIN McCARTHY, California
BILL POSEY, Florida
LYNN JENKINS, Kansas
CHRISTOPHER LEE, New York
ERIK PAULSEN, Minnesota
LEONARD LANCE, New Jersey

JEANNE M. ROSLANOWICK, *Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

DENNIS MOORE, Kansas, *Chairman*

STEPHEN F. LYNCH, Massachusetts
RON KLEIN, Florida
JACKIE SPEIER, California
GWEN MOORE, Wisconsin
JOHN ADLER, New Jersey
MARY JO KILROY, Ohio
STEVE DRIEHAUS, Ohio
ALAN GRAYSON, Florida

JUDY BIGGERT, Illinois
PATRICK T. MCHENRY, North Carolina
RON PAUL, Texas
MICHELE BACHMANN, Minnesota
CHRISTOPHER LEE, New York
ERIK PAULSEN, Minnesota

CONTENTS

	Page
Hearing held on:	
September 28, 2010	1
Appendix:	
September 28, 2010	23

WITNESSES

TUESDAY, SEPTEMBER 28, 2010

Caruso, David B., Chief Executive Officer, Dominion Advisory Group	11
Comras, Victor D., Special Counsel, The Eren Law Firm	5
Landman, Stephen I., Director, National Security Law and Policy, The Investigative Project on Terrorism	7
Lewis, Eric L., Partner, Baach Robinson Lewis	9

APPENDIX

Prepared statements:	
Minnick, Hon. Walt	24
Caruso, David	28
Comras, Victor D.	32
Landman, Stephen I.	52
Lewis, Eric L.	69

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Moore, Hon. Dennis:	
Written statement of Simon A. Charlton	78

A REVIEW OF CURRENT AND EVOLVING TRENDS IN TERRORISM FINANCING

Tuesday, September 28, 2010

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

The subcommittee met, pursuant to notice, at 4 p.m., in room 2128, Rayburn House Office Building, Hon. Dennis Moore [chairman of the subcommittee] presiding.

Members present: Representatives Moore of Kansas, Lynch; Biggert, and Paulsen.

Also present: Representative Minnick.

Chairman MOORE OF KANSAS. This hearing of the Subcommittee on Oversight and Investigations of the House Financial Services Committee will come to order.

Our hearing today is entitled, "A Review of Current and Evolving Trends in Terrorism Financing." This is our 18th O&I hearing in the 111th Congress.

We will begin this hearing with members' opening statements, up to 10 minutes per side, and then we will hear testimony from our witnesses.

For our witness panel, members will each have up to 5 minutes to question our witnesses.

The Chair advises our witnesses to please keep your opening statements to 5 minutes so we can get to members' questions. Also, any unanswered question can always be followed up in writing for the record.

Without objection, all members' opening statements will be made a part of the record. And I now recognize myself for up to 3 minutes for an opening statement.

Today's hearing is the third in a series of hearings focused on the very important issue of combating terrorism financing and money laundering. Earlier this year, the subcommittee held a hearing reviewing several oversight reports by GAO and the Treasury Department's Inspector General that examined FinCEN's efforts with respect to suspicious activity reports, Bank Secrecy Act compliance, and anti-money laundering, among other issues.

This subcommittee held another hearing reviewing the Treasury Department's efforts to combat the financing of terrorism while also reviewing various controls, disclosure, and decision-making processes to ensure law-abiding individuals and charities receive adequate due process.

With today's hearing, we are taking a step back and looking at the broader issue of global terrorism financing in general. For example, how is terrorism being financed today, and how are terrorist organizations altering their financing techniques to avoid current efforts by the U.S. Government to stem the flow of money to terrorists? What are the latest trends our government needs to pay attention to so that we are making every effort to eliminate the financing of terrorism?

I look forward to hearing from our panel of nongovernment witnesses who come to the table with a variety of perspectives to help provide a fresh look at these difficult questions.

The May 1st Time Square bomb attempt earlier this year is a vivid remainder that despite a long period of time passing, over 9 years now since the tragic September 11, 2001, terrorist attacks, there remain those who wish to do us harm. And our government should remain vigilant in shutting those terrorist groups down, including stopping the financing that supports them.

This week, the Obama Administration announced plans to require U.S. banks to report all electronic money transfers into and out of the country to the authorities with the aim of helping the government better track the kind of money transfers that helped finance the al Qaeda hijackers on 9/11. We must keep in mind that the government has limited resources, and we will want to review that plan to ensure it is properly analyzed in the days and weeks ahead.

Should the government take other steps to better combat the financing of terrorism? I look forward to hearing from our witnesses to explore this issue further.

I now recognize for 4 minutes the ranking member of this subcommittee, my colleague and friend from Illinois, Ranking Member Judy Biggert.

Mrs. BIGGERT. Thank you, Mr. Chairman, and thank you for scheduling today's important hearing. It is clear that terrorists will stop at nothing to raise funds and funnel money to harm our citizens and our way of life. They will use any means possible—credit card fraud, travelers checks, and Internet payment systems—to carry out their attacks. I am very concerned that terrorists continue to exploit formal and informal financial systems to move amounts of money ranging from thousands to upwards of billions of dollars. Terrorists are nimble at adapting to an ever-changing marketplace, trying to keep one step ahead of financial institutions, regulators, and law enforcement.

Are the efforts of financial institutions, the regulators and law enforcement sufficiently vigilant and agile to track and dismantle terrorist financing and ultimately shut down terrorist operations? Should certain efforts be reformed, better targeted, and streamlined?

According to today's witnesses, I think we will learn that there certainly is room for improvement. Improvement is not solely the responsibility of one regulator, one financial institution or one law enforcement entity. It is everyone's responsibility to stop the financing of terrorism. National security should be at the top of everyone's agenda, and failure to do so is unacceptable.

Finally, the United States cannot do this alone. We must strengthen partnerships and commitments from the international community to bolster antiterrorist financing operations. So I look forward to hearing from today's witnesses, and I yield back.

Chairman MOORE OF KANSAS. Thank you.

Next, the Chair recognizes Mr. Lynch from Massachusetts for 2½ minutes.

Mr. LYNCH. Thank you, Mr. Chairman, and Ranking Member Biggert, for holding this hearing.

I would like to welcome the witnesses and thank them for their willingness to help the committee with its work. As the cochairperson of the Task Force on Terrorist Financing and Anti-Proliferation, I sent along with my colleague Mr. Castle of Delaware a letter to the chairman back in May expressing an interest in holding a hearing that would focus on the development and growth of the informal banking system. We have seen one recent example of this system in the case of the Times Square bombing.

Since the bombing attempt occurred over the summer, we have learned that Faisal Shahzad attained transfers of $5,000 and $7,000 which were provided by an informal money system known as a hawala. Hawalas or hundis, as they are sometimes known, operate apart from the regulatory grid. Terrorist organizations have exploited the informal nature of the hawala structure to move cash across borders and to fund their illicit activities.

Despite the certain success of our enforcement agencies in preventing the use of the formal banking system by terrorist groups, we need to know more about informal transfer systems like these hawalas that allow operations to continue.

I had an opportunity to read over the testimony of each of our witnesses last night. And I look forward to and welcome their thoughts and suggestions in terms of how we might have greater success against these informal money transfer systems. Again, I thank you for your willingness to help the committee with its work, and I yield back the balance of my time.

Chairman MOORE OF KANSAS. Thank you, sir.

The Chair next recognizes Mr. Paulsen from Minnesota for 4 minutes.

Mr. PAULSEN. Thank you, Mr. Chairman, and Ranking Member Biggert, for holding this important hearing as well today.

We know that financial institutions often serve as the first line of defense in detecting financial crimes and providing critical information to law enforcement. The ability to follow the money trail provides our intelligence and our law enforcement community with information that leads to a broader understanding of terrorist organizations and drug dealers. And certainly, the laws that passed in Congress since 9/11 have been crucial in helping to obtain that information. It is essential to catching criminals and defeating terrorists.

But we must be vigilant and make sure that we can to continue to provide the necessary tools.

In light of the President's proposal earlier this week to monitor all electronic money transferrings that are coming in and out of this country, I am interested in hearing more about how we can

make improvements in tracking terrorist financing from the panel today .

And I want to thank the witnesses. I look forward to the testimony and making proposals that we achieve some additional success.

Mr. Chairman, I yield back.

Chairman MOORE OF KANSAS. Thank you, sir.

The Chair now asks unanimous consent for Representative Walt Minnick to participate in today's hearing and give a brief opening statement. Without objection, Mr. Minnick, you are recognized for up to 3½ minutes, sir.

Mr. MINNICK. I thank you, Chairman Moore and Ranking Member Biggert. I commend you for holding this important hearing today and I thank you for the opportunity to participate.

As 9/11 illustrated with jarring clarity, disrupting the financing of global terrorism is critically important to the survival of civilized society. On this, the 9th anniversary of this tragedy, we need to examine the progress that has been made and the shortfalls in the international financial surveillance system that are yet to be addressed.

Just how vulnerable is our banking system today to being the conduit through which sophisticated global terrorist groups finance their infrastructure and procure their weapons of death and destruction? How are we doing in identifying and using financial information to disrupt related endeavors such as drug trafficking, weapon sales, sanction breaking, and the money laundering incident to other large-scale criminal activity?

We hope and expect that our witnesses today will give us some of the answers.

The committee has previously discussed the lack of oversight of massive fund flows originating in the Middle East. It has studied the interconnectiveness of global financial centers. It has explored the threats posed by banking secrecy rules in Switzerland, the Caribbean, and emerging financial centers of the Far East. It has argued the trade-offs between maintaining privacy and disclosing threats to international security.

We are here today to learn whether the U.S. financial authorities have the tools, staffing, and the will to successfully perform our Nation's portion of this task: to discover whether foreign governments and international financial institutions are similarly focused and effective; and to understand whether this information is being shared and effectively used to arrest and imprison drug kingpins, foil al Qaeda and other international terrorist groups, enforce trade sanctions, and identify global criminal activity.

Do we understand our vulnerabilities, and are we working effectively to overcome them? These are all questions that must be answered to assure our citizens that our government is protecting both their assets and our Nation's security in an increasingly dangerous and interconnected world.

Thank you, Mr. Chairman. I yield back.

Chairman MOORE OF KANSAS. Thank you, Mr. Minnick.

I yield myself an additional minute.

Before our witnesses testify, I want to put today's testimony in the proper context. I am—and I hope all of us are—most interested

in learning about the latest trends in terrorist financing and/or money laundering, so that we can make sure our government is adapting and is fully prepared to keep up with them.

There are some allegations in the written testimony where parties not present are named and accused. We are not a court of law, and we cannot engage in factfinding in this setting. We do not have all the facts or the response—if we don't have the response of those named. Opinions expressed and allegations made must be viewed within that context, and we will leave the record of the hearing open to afford any party named an opportunity to present their own response and their side of the story.

I am pleased now to introduce our panel of witnesses this afternoon. First, Mr. Victor Comras, special counsel of the Eren Law Firm. Mr. Comras is a retired career U.S. diplomat, having served 35 years at the State Department before being appointed by then-United Nations Secretary General Kofi Annan to serve as one of five international monitors to oversee the implementation of Security Council measures against al Qaeda and tourism financing.

Second, Mr. Stephen Landman, director of national security law and policy at the Investigative Project on Terrorism. Mr. Landman has researched and written extensively on issues related to terrorist support structures with a focus on financing and the use of developing technologies by terrorist groups.

Third, Mr. Eric Lewis, partner at Baach Robinson Lewis, where he has represented clients in a variety of complex legal cases, many involving financial fraud. Mr. Lewis previously served for many years as an adjunct professor of law at Georgetown University.

And finally, Mr. David Caruso, chief executive officer, Dominion Advisory Group. Mr. Caruso began his career as a Special Agent with the U.S. Secret Service before being hired to manage the Anti-Money Laundering and Enhanced Due Diligence Group at JPMorgan. He subsequently served as a director at two Big Four accounting firms, where he led anti-money laundering compliance and fraud investigations and has more than 15 years of experience creating and implementing comprehensive anti-money laundering or AML programs.

Without objection, your written statements will be made a part of the record.

Mr. Comras, sir, you are recognized for 5 minutes.

STATEMENT OF VICTOR D. COMRAS, SPECIAL COUNSEL, THE EREN LAW FIRM

Mr. COMRAS. I am here today to express my views and concerns with regard to U.S. and international efforts to stem the flow of financial support to terrorist organizations.

As mentioned, we have just passed the 9th anniversary of that terrible 9/11 attack that confirmed for us and for most of the international community that international terrorism poses one of the gravest threats to international peace and security.

Since then, governments have spent well into the hundreds of billions of dollars to prevent, defend against, and fight terrorism, and to provide security for their interests at home and abroad. And the world's financial community has invested billions more on regulatory compliance measures to police accounts and transactions in

order to steer clear of counterterrorism and money-laundering issues.

Yet, terrorism continues to poses a worldwide threat. Empirical evidence demonstrates that al Qaeda, the Taliban, Hamas, Hezbollah, and other terrorist groups continue to have access to the funds they need to maintain their organizations and their terrorist operations. And if anything, Taliban funding is expanding, not diminishing.

The Taliban's cash flow from Afghanistan's poppy fields comes as no surprise, but the $106 million they reportedly received last year from overseas donors is a real eye-opener.

Hamas and Hezbollah have also developed their own worldwide financial network, drawing closely on their links with the Muslim Brotherhood. These terrorist groups have also tapped into criminal networks operating in the tri-border area of Latin America, and in West Africa and Southeast Asia. And this transfer of money from criminal activities to terrorism relies heavily on money-laundering techniques here and abroad.

I know, Mr. Chairman, that our U.S. financial institutions take the threat of international terrorism very seriously. They have come a long way since 9/11 in putting in place effective procedures to identify reporting to block suspicious transactions, and the U.S. Government regulatory agencies are now both intensive and vigilant in their oversight.

But while great strides have been made in cutting down the flow of terrorism funds from the United States, our banks remain awkwardly vulnerable to getting caught up in terrorist group-related transactions that originate and terminate overseas. Our banks have little choice but to rely on the veracity and accuracy of the transactional information provided to them by their overseas clients and associates. And in the fast and very competitive world of international financial transactions, these assurances are often shortchanged.

The problem is further complicated by the emergence overseas of numerous underfunded and underregulated homegrown banks and informal transfer facilities that lack the wherewithal to mount and maintain an effective compliance system. And many of these financial institutions are located in areas quite susceptible to the recruitment of terrorists.

It is essential, therefore, that there be greater cooperation between the U.S. Government in sharing cautionary information that they acquire through their own channels and alerting their banks, our banks, to such suspicious transactions; not just to rely on the one-way flow of information from the banks to the government that seems to exist today.

When I say that the locus of terrorism financing problem is largely overseas, I do so with a caveat. As you know, there have been several actions recently to penalize financial institutions, foreign financial institutions with branches in the United States, for their involvement in dollarizing terrorist-related transactions. There have been other egregious cases where foreign bank branches in the United States have sought to circumvent our sanctions laws and regulations.

And when we take these stringent actions against them, we send a strong message that the United States will not countenance such activities in the United States.

And Mr. Chairman, an even stronger message is now being sent by victims of terrorism as they move in U.S. courts to hold these and other financial institutions accountable for facilitating the flow of funds to terrorist organizations.

We must face up to the fact, Mr. Chairman, that while we take seriously the illegality of all transactions that support terrorism in their activities, many other countries do not. Many of the transactions that these banks have engaged in are not considered illegal in many of the other countries in which they operate.

I can tell you that shortly after 9/11, you may recall the Security Council adopted resolution 1373, which was meant in part to obligate all countries to prevent the transfer of funds to terrorist organizations for any terrorist purposes. But that resolution has a serious loophole; it fails to define terrorism. Rather, it leaves to each country to decide for itself which groups they consider terrorists and which they hail as freedom fighters.

The fact is that there is only really a very small fragile and narrow international consensus as to who the terrorists are. For the most part, it is represented in a small list of designated al Qaeda and Taliban entities and individuals that has been published by the United Nations. I want to make it clear; beyond that point, beyond that list of designated individuals and entities, there is no international consensus and, therefore, no clear and enforceable international obligation which inhibits countries from allowing their financial institutions to engage in financial transactions with such undesignated individuals and entities. Given U.S. bank interaction with this larger international—

Chairman MOORE OF KANSAS. The gentlemen's time has expired. Will you please wind up?

Mr. COMRAS. —banking community, the vulnerabilities become stark. And we must be extra vigilant when it comes to ensuring the information regarding the originator and ultimate recipient of each transaction is complete and accurate.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Comras can be found on page 32 of the appendix.]

Chairman MOORE OF KANSAS. Thank you, sir.

Mr. Landman, you are recognized for up to 5 minutes, sir.

STATEMENT OF STEPHEN I. LANDMAN, DIRECTOR, NATIONAL SECURITY LAW AND POLICY, THE INVESTIGATIVE PROJECT ON TERRORISM

Mr. LANDMAN. Thank you, Chairman Moore, Ranking Member Biggert, and distinguished members of the subcommittee. Thank you very much for holding today's hearing on the evolving threat of terrorist financing.

In the past decade, the speed with which the United States has developed, implemented, and fine-tuned its counterterrorist financing strategy has been nothing if not impressive.

Despite these successes, however, terrorist groups continue to raise and move money for recruitment, indoctrination, logistical

support, training, and to finance their murderous actions. As we are learning, however, like the terrorist groups, their financing crosses both geographical borders and technological boundaries. Indeed, like water on concrete, this money is finding all of the holes.

Through a combination of criminal prosecution, regulatory enforcement, and civil litigation, the United States has effectively closed off the formal financial sector to terrorist groups. At the forefront of the regulatory reforms are amendments to the BSA that accompany the PATRIOT Act. These updated recordkeeping and reporting requirements have expanded both the depth and breadth of financial intelligence available to law enforcement officials.

And while the result has been a more secure financial system, it could benefit still from greater cooperation between law enforcement and the private sector. And although the idea has been proposed before, I would again urge the committee to consider working to increase information sharing between banks and law enforcement officials by granting bankers access to limited classified information.

But no amount of regulations will matter for those banks that are intent on supporting terrorism. And that is why Congress must act to clarify the scope of financial services under the material support law. American victims of terrorism have been working to hold institutions like Arab Bank liable for providing what amounts to death insurance plans by Hamas to Hamas militants. And in each of the cases, the institutions have responded that they were simply providing routine banking services, conduct that they argued was not prohibited. Congress can reaffirm that there is nothing routine about terrorism and by amending the term Financial Services to encompass "routine banking services."

While these steps will ensure that terrorists remain persona non grata in the banking industry, FTOs continue to raise and move money through the abuse of charitable institutions and underground banking. The shuttering of the Holy Land Foundation, an Islamic charity proven to have provided over $12 million to Hamas, demonstrates that terrorist groups are able to raise money for acts of violence and that they are willing to do so under the guise of humanitarian relief efforts.

Today, Viva Palestina, a British-based charity with an American branch, has picked up where HLF left off, flouting U.S. terror finance laws and raising over $200,000 in the United States and providing that money to Hamas in support of humanitarian efforts.

In order to ensure the sanctity of the charitable sector, Congress should resist any efforts that would create a humanitarian aid exception to the material support law. And you can also urge expanded review and verification of charitable filings for inconsistencies.

Another tried-and-true method for moving terrorist finances has been the underground banking system, specifically hawalas. And despite expanded applicability of the BSA to cover hawalas, the statute must be more aggressively enforced.

The recent arrest of Mohammed Younis, who allegedly helped finance the failed Time Square bombing by serving as a hawaladar is a reminder of the importance of financial investigations as part

of a broader counterterrorism policy. Every terrorism investigation should have a parallel terror finance component.

Finally, moving forward, we must recognize that rather than simply rest on their laurels, terrorist groups have shown an incredible ability to adapt changing technologies to their needs. The creation of stored value cards and the expansion of the Internet are just two of the problems that those tasked with countering terrorist financing will face over the next decade.

If you are a terrorist, technology has made bulk cash smuggling easier than ever in the form of stored value cards. And although they bear all of the requisite qualities, they are not currently considered monetary instruments subject to regulation. The exclusion of them as reportable instruments is the result of technology outpacing regulations. And while reports suggest that Treasury is currently considering adding those to the list of monetary instruments, they must act quickly to plug this gap before terrorist financiers take advantage of it.

More worrisome, however, is the Internet, which has already revolutionized FTO operations, from the spread of propaganda to the planning and preparation of attacks. And a particular concern should be virtual worlds, which have the capacity to serve as the hawalas of the 21st Century. They provide many of the same characteristics as the existing hawala networks; they are fast, inexpensive, reliable, convenient, and, most notably, discreet. The existing regulations should be updated to curb the potential for the abuse, bring virtual worlds under the umbrella of covered institutions under the BSA.

Members of the committee, American efforts to disrupt terrorist financing schemes have put organizations such as al Qaeda in dire financial straits. These successes however have been tempered by continuing blind spots in the enforcement of existing regulations and an inability to update current laws on pace with technological advancements.

Chairman Moore, thank you very much for allowing me to come and speak with you today. I look forward to your questions on this critical issue, and I yield back the balance of my time.

[The prepared statement of Mr. Landman can be found on page 52 of the appendix.]

Chairman MOORE OF KANSAS. Thank you, sir.

The Chair next recognizes Mr. Lewis for up to 5 minutes.

STATEMENT OF ERIC L. LEWIS, PARTNER, BAACH ROBINSON LEWIS

Mr. LEWIS. Thank you, Chairman Moore, Ranking Member Biggert, and the distinguished members of the subcommittee for the opportunity to testify today regarding one of the largest abuses ever of the United States banking system. The fraud and money-laundering scheme that I would like to discuss involves the transfer of approximately $1 trillion through the United States financial system, all directed by a single Saudi national named Maan Al-Sanea, using a Saudi Arabian remittance company or hawala called the Money Exchange, as well as two banks he controlled in Bahrain and other companies in the Cayman Islands and Switzerland.

The fraud appears to have deprived its victims of more than $20 billion, making it larger than the Madoff fraud in actual out-of-pocket loss, yet there were no questions asked, not by banks, regulators, or prosecutors, until the whole scheme collapsed.

The Money Exchange's main U.S. dollar account was with an American bank in New York. The Money Exchange was a small company with a transactional volume for its remittence customers of around $60 million per year in total. Nevertheless, it approached a major U.S. bank that visited it in the Middle East and said it would like to open a corresponding account in New York in order to transfer approximately $15 billion in payments annually.

At least four huge red flags present themselves right at the outset, which is the key point at which banks can make determinations about the bona fides of their customers: first, you have a high-risk region and country, the Middle East, Saudi Arabia; second, a business that accepts money transfers for walk-in customers, with whom it has no account relationship and does none of the necessary due diligence; third, you have a massive transactional volume, $15 billion a year; and fourth, you have a volume of transactions which is entirely disproportionate to the customer's ostensible business.

One would expect a searching interrogation of this customer; that is what the "know your customer" rules require. There should be a careful evaluation of the intended use of the account, the source, destination, and business purpose of the funds flowing through. And because the prospective customer is itself a financial institution, there must be a thorough investigation of that institution's anti-money laundering and "know your customer" policies, yet our investigation has revealed no evidence of any significant due diligence or anti-money laundering investigation of the Money Exchange in Saudi Arabia.

The two Bahraini banks, Awal Bank and the International Banking Corporation, had no legitimate customers. They were created and used by Mr. Al-Sanea to borrow money and then funnel it through the U.S. financial system to dummy customers and then to his own companies. So if the core is to know your customer's customers, here you had two large banks that had no customers.

U.S. anti-money laundering and anti-terror finance policy is a two-part defense. There must be pre-event diligence by the banks, backed by regulatory oversight, and post-event law enforcement, where the initial diligence has failed to prevent or detect money laundering.

Banks are the critical first lines of defense, supported by clear regulation. But banks often have incentives to look the other way, and fines for noncompliance are still viewed as relatively unlikely to occur as the cost of doing business if they do. This must change if the system is to work effectively.

Our regulatory regime also needs to make it clear that if banks agree to open dollar accounts for customers, it doesn't matter if the relationship is based elsewhere. That customer must be subject to all of the scrutiny and rigor applied to someone who walks off the street in midtown Manhattan to open a bank account. We are not aware of any investigations ongoing by the relevant regulator into this massive systemic failure. We understand that Congressman

Peter King has written to the attorney general to request an investigation, but we have received no information or requests for information to date from the Justice Department.

The United States alone possesses the resources and the tools to protect the global financial system from international financial crime, money laundering, and terror financing. And the United States has an overwhelming national security interest in taking the lead. We cannot delegate this critical responsibility to others. This fraud involved more than a dozen countries. Each of them had only a piece of it. Each can claim that it can only investigate and see a slice. Each can claim some other country has a greater responsibility. But in an age when international fraudsters and money launderers can cross borders with a click of a mouse, the response cannot be, "It is not our responsibility." That is a recipe for disaster.

Banks must diligently inquire into their customers and their customers' customers. Wrongdoers must be investigated, charged, extradited, and prosecuted. The United States must lead, but cooperation must be sought. Saudi Arabia, for example, is a committed ally in the fight against terror financing, and I have no doubt if the United States underlined the importance of getting to the bottom of this or other massive money-laundering schemes that originate there, the Saudis would cooperate.

Extensive legislation is not needed; the need is for strong oversight and firm priorities, together with clearly defined responsibilities and accountability.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Lewis can be found on page 69 of the appendix.]

Chairman MOORE OF KANSAS. Thank you, sir, for your testimony.

Mr. Caruso, you are recognized for up to 5 minutes, sir.

STATEMENT OF DAVID B. CARUSO, CHIEF EXECUTIVE OFFICER, DOMINION ADVISORY GROUP

Mr. CARUSO. Good afternoon, Chairman Moore, Ranking Member Biggert, and members of the subcommittee.

Thank you for the opportunity to appear before you today to discuss the vulnerabilities of our financial system to terrorists and money launderers. Financial institutions, particularly depository institutions, play a crucial role in identifying and reporting terrorist financing and money laundering.

Over the last 10 years, banks have spent considerable amounts of money to hire staff and implement software systems to detect suspicious activity. As a result, most financial institutions comply with the Bank Secrecy Act, or BSA. However, compliance with regulations and identifying potential terrorist financing and money laundering are not necessarily synonymous.

Suspicious Activity Reports, or SARs, reporting activity related to BSA violations account for nearly half of all SAR filings. The majority of these SARs are made up of those reporting attempts to evade the Currency Transaction Reporting threshold, a practice known as structuring. The burden of detecting, investigating, and reporting cash structuring using today's version of the SAR hampers a financial institution's ability to identify transactions associ-

ated with more serious crimes and makes our financial system more vulnerable to terrorist financing and money laundering.

Consideration should be given to creating a new SAR, designed to report only cash structuring. Such a SAR would still provide the government with required information and would reduce the time and effort needed by institutions to complete the form, thus enabling more energy to be directed at uncovering terrorist financing and significant money laundering.

When institutions detect structuring, they must adhere to the requirements of the Federal Financial Institutions Examination Council and FinCEN which mandate that SARs include a thorough and complete narrative or written depiction of the events that led to the conclusion a SAR must be filed. In addition, institutions are expected to compile supporting case information into a comprehensive file. This information is used by auditors and examiners as a way to test a bank's compliance with BSA.

Over the past 5 years, the expectations of regulators and industry practice has expanded. Writing the SAR narrative is as time-consuming as ever. A modified SAR to report structuring will convey the relevant facts of an investigation—who, what, where, when, and how much—but can be compiled into a more concise format, such as a table or spreadsheet, that will still inform law enforcement of what it needs to know, provide regulators with evidence of an institutions's compliance with the BSA, and then free up resources of a bank to focus on detecting terror financing and sophisticated money-laundering schemes.

Financial institutions struggle with how to effectively detect terrorist financing. Retrospective analysis of terrorist funding does not provide clear enough direction to bank investigators on what specific transactions may indicate funds are being sent to support terrorists. Depository institutions and other financial institutions, including money services businesses, have implemented automated software systems designed to more effectively and quickly identify suspicious activity. However, these software systems produce large numbers of alerts mostly related to structuring because structuring is the easiest type of activity for these systems to identify. Satisfying the regulatory requirements around investigating, documenting, and reporting structuring takes a typical bank investigator between 3 to 8 hours.

Our experience working with small, mid-sized, and large banks shows us that structuring accounts for between 60 and 70 percent of all BSA-related SARs. We also see that over half of the customers who structure have neither structured before nor subsequently to the incident in question. These one-time structurers, however, eat away at the time a bank staff can then spend uncovering and investigating activity whose impact on the financial system and national security could be much more serious.

Structuring SARs provide the government with important information, including information that may lead to the discovery of serious criminal activity. The importance of this information should not be minimized. What should be minimized, however, is the time and effort needed to report the activity.

By creating a SAR tailored to report only structuring, the government would relieve financial institutions of their largest BSA, AML

compliance burden and then enable institutions to use that available time and those available resources to identify and report more serious crime. Thank you, again, for the opportunity to testify here today.

[The prepared statement of Mr. Caruso can be found on page 28 of the appendix.]

Chairman MOORE OF KANSAS. Thank you, sir.

I appreciate the testimony of the witnesses.

I am going to start the questions.

The first question, Mr. Caruso, is directed to you. I agree with and appreciate your testimony where you commend U.S. financial institutions for working with the government to combat terrorism financing as well as the government's vigilant efforts to stem the flow of money to terrorist organizations.

I don't know if you saw the announcement yesterday, but do you have a general reaction to the Administration's plan to expand tracking of electronic money transfers? Is this a wise approach, or does it raise concerns?

Mr. CARUSO. It does raise concerns, from my perspective, knowing how difficult it is for institutions to comply with existing rules and regulations, as mightily as they do try. And our experience is that nearly all do try as best they can.

But in order for a bank to capture that information, and report it to the government on a regular basis, although I understand the government's view that there are only 300 or 400 banks that it will impact, will be a significant burden on those banks. And then it raises for me the question that my testimony raises, is that the best use of a bank's time to report that information?

Chairman MOORE OF KANSAS. All right, thank you.

Mr. Landman, do you have any thoughts about this question?

Mr. LANDMAN. I saw it yesterday, and I have been thinking about it since.

My immediate thought was that it seemed like a good idea. That being said, I think there are significant concerns with the volume of data that it is going to result in. Banks are going to be giving way more information to the government. And the same way that Mr. Caruso suggests it may overwhelm banks, I think it may have the effect of overwhelming the government. But if the government can figure out a way to work with banks and filter that properly, it would be very good.

Chairman MOORE OF KANSAS. Any thoughts, Mr. Comras?

Mr. COMRAS. I think the filtering is the critical element.

Chairman MOORE OF KANSAS. Turn your microphone on, please, sir.

Mr. COMRAS. Sorry.

I think that filtering is the critical element. The mass of information is sometimes the easiest way of hiding the real gems in the information. And until we know exactly what we want to target and have a better profile and direct our efforts towards that profile, a lot of our efforts are going to be wasted.

Chairman MOORE OF KANSAS. Thank you, sir.

Mr. Caruso, I am intrigued by a concern Mr. Lewis raised on page 6 of his testimony, that compliance officials are viewed as "anti-business." Have you found this to be the case? And what

steps could the government take to encourage self-policing by financial firms, going beyond the minimal requirements and encouraging a culture within firms to remain vigilant against new terrorism financing techniques?

Mr. Landman?

Excuse me, Mr. Caruso, first.

Mr. CARUSO. I think that it is a fair assessment that compliance departments are viewed by the lines of business as often impediments. However, I don't necessarily view that as a bad thing. I think a natural tension between a business group and compliance group is actually important because it makes the compliance staff perform their job better, to argue their case about how a customer should be treated or a transaction should be reported. And that process, in all of my experience, actually helps educate the business people better than if the compliance people were to have some sort of carte blanche and just be able to dictate what can happen.

Chairman MOORE OF KANSAS. Any thoughts, Mr. Landman?

Mr. LANDMAN. There is an easy response which is just that I understand that this is burdensome, but there are legitimate civil penalties that would be enforced if we don't do this work. And from the perspective of the compliance department, they are just saving the bank money long term in litigation. Look at the case of Arab Bank, this case, which may litigate for 10 more years could wind up costing our bank hundreds of millions of dollars; that is something worth protecting.

Chairman MOORE OF KANSAS. Thank you, sir.

Mr. Comras, you make some strong points in your testimony that beyond international consensus to combat the financing of al Qaeda and the Taliban, the international community has not reached consensus to stem the flow of money to other terrorist groups. What actions should the United States Government take in response to this concern?

Mr. COMRAS. Mr. Chairman, I think our response has to take two directions. One, we have to use the leverage that we have through our banking community and the major role that we play to alert other banks to the risks that are involved.

At the same time, we have a very major leverage with the Antiterrorism Act of 1996, which allows victims of terrorism to use our courts to hold banks, even those that are outside the United States, accountable when they are involved in the financing of terrorists that caused such victims to suffer from terrorism.

The second route we must take is to work through the international organizations, through FATF and through other forums, to convince our friends and allies to take this risk seriously. I had an opportunity to look very closely at this issue over the last couple of years and I wrote a book on that trying to devote greater attention to using the international institutions to deal with a developing consensus, including a definition of terrorism that is more universal and has applicability to all of these banks.

Chairman MOORE OF KANSAS. Thank you, sir.

The Chair's time has expired. The Chair next recognizes Ranking Member Biggert for up to 5 minutes.

Mrs. BIGGERT. Thank you, Mr. Chairman.

It seems that nearly every time a bank is fined for having a bad anti-money laundering program, we find it has received passing evaluations of its money-laundering program during the period that was in question. How is it that banks are able, unintentionally or otherwise, to facilitate the flow of large sums of money to or for customers when they really don't know anything about the customer without regulators picking that up? Are regulators and bank examiners properly trained or just not doing their jobs?

Maybe, Mr. Comras, could you start with that?

Mr. COMRAS. Banks, of course, are very reliant on the information that is provided to them by their clients overseas, and they, I think, have taken for granted that some of these clients are not providing all of the information that is required. We now require a whole set of information with respect to transactions that includes identification information of the originator and the recipient of transactions. Other banks have not had that practice, and only a few banking jurisdictions, and I include Europe, require such information to accompany transfers.

We have to develop a better system to assure ourselves that the transactional information that is provided by the overseas banks is accurate. And in cases where it is not, take very firm action to deal with that situation.

Mrs. BIGGERT. Do you think that the banking regulators share in the responsibilities for gaps in our financial institutions?

Mr. COMRAS. I think that the banking regulators look very closely at the information that is provided, and they take that information, use it, run it through their filters, run it through the software, run it through their name checks. But they also are prisoners of a system that relies so heavily on the information that is provided. And until you have some alarm that is set off, some incident where you know that you have gotten false information, there is not much that you can do to check that information.

That is why I think it is important that there be a better sense of cooperation between government entities or information-gathering entities and banks to assure that there is a greater flow to the banks of information that can give them the caution that they need to take a closer look when they are getting information from overseas banks.

Mrs. BIGGERT. Thank you.

Mr. Landman, would you agree with that, that the regulators are—

Mr. LANDMAN. Absolutely, Ranking Member Biggert. I think through the FATF, we can ensure that foreign financial institutions are implementing the same type of "know your customer" requirements that are used here. And I think that through something I mentioned in my testimony, the increased cooperation with law enforcement perhaps by providing classified briefings to banks, they would be able to get that kind of detail that Mr. Comras suggested is going to be necessary.

Mrs. BIGGERT. There was so much concern with the PATRIOT Act that the different groups couldn't talk to each other. Do you find that really has changed now, so law enforcement has been able to talk the regulators and the banks?

Mr. LANDMAN. I think that right now, it seems like it may be information going one way from banks going towards the government. At least, that is the view that I have seen of it. I think that the banks could probably benefit from this additional information from the government. And I think the government would benefit as well. There would be more precise reporting in the future as a result of that.

Mrs. BIGGERT. All right. Do you think that the system in place to identify and stop the terrorist financing is flexible enough to evolve as the threats change, or does the apparatus become static—

Mr. LANDMAN. I hope so. I hope it is flexible enough. I think that everything that I have spoken about today are minor tweaks. We are not talking about major changes to the Bank Secrecy Act. We are not talking about major changes to any of the FinCEN regulations. And I think that through minor tweaks, you can continue to use the same regulations moving forward.

Mrs. BIGGERT. Mr. Caruso, how effective has FinCEN or OFAC or the Treasury Department been in providing the financial institutions with the information necessary to combat terrorism?

Mr. CARUSO. I think that it has been modest, the success has been modest, that the information that the government is able to provide institutions. Institutions struggle amongst themselves on how to identify the types of activities that the witnesses have spoken about here today and that the members are so interested in.

I think regulators are very process-oriented. They look at a bank to make sure they have all the mechanics and logistics of an anti-money laundering program in place, but without specificity on what exactly to look for—Mr. Landman, I thought, made an excellent suggestion—that if law enforcement were able to inform regulators very specifically about the types of criminal investigations and intelligence investigations that they have ongoing, the regulators would have a much, much better understanding of what it is that the banks—what they should be looking for at banks, and then, subsequently, banks will begin to look for those things.

Mrs. BIGGERT. Thank you, I yield back.

Chairman MOORE OF KANSAS. Thank you to the gentlelady.

The Chair recognizes Mr. Lynch for up to 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman.

Mr. Caruso, you raised the issue about the cumbersome and time-consuming nature of the SARs reporting. Right now, I think banks file about 1.4 million SARs per year, so we have to go through those to try to get information. They also file, I think, 14 million CTRs, which are for transactions over $10,000. And now, this morning, I read in the New York Times and the Washington Post that the Obama Administration intends to expand its counter-terrorist financing efforts by requiring U.S. banks to report all international money transfers. From your end, workability, what do you think that expansion is going to do to your ability to report in a timely fashion and to handle the volume of reports that will be necessary?

Mr. CARUSO. Banks are going to have to hire more people. They are going to have to develop additional systems to capture the information that their other technology systems capture. They will

have to develop a lot of processes and procedures to report that information.

And I would imagine that the government would hold the view that if the bank is capturing this information and reporting it to the government in a way that they have not yet done before, there would be an expectation that the bank will look at the information.

Mr. LYNCH. Just thinking about the huge volume of information that is going to be coming into the government, and then we are going to have to review that to find out—to actually use the information rather than just collecting it. I am just concerned about whether or not this is the best use of our time and the most efficient use of the information that we are getting.

Is there a way—you talk about the fact that 60 to 70 percent of the SARs right now are these structuring noncompliance situations, is there a way to speed that up where it is—there is a lot of similar information, so that you can spend more time on the more serious offenses? Is there some way we might streamline that?

I know Mr. Shaul from Mr. Frank's committee has indicated there might even be a way to bar code some of these reports or some portion of the information, just so that bank employees aren't spending all their time doing this.

Mr. CARUSO. Yes. The way the industry understands the problem is that the government's computers are unable to accept what most would consider a very simplistic and modern form of communication, the spreadsheet, and we have all seen them, in which valuable information can be captured almost instantaneously, compiled and reported within minutes. Unfortunately, the requirements now dictate that a bank's employees create a narrative and, in essence, tell a story around this very simplistic event.

Mr. LYNCH. All right. I only have a minute and a half.

Mr. Comras, we are sort of—there is a double-edged sword here. Initially, I worked a lot with FinCEN in Afghanistan, in Jordan, in Tunisia, and in Morocco, setting up Financial Intelligence Units. Some countries it appears—this is my opinion—set up these FIUs in order to get off the bad list. In other words, they wanted to be compliant with—after September 11th, they wanted to show that they were doing something to stop this. But the number of SARs and reports that we are getting are very limited from a lot of these countries. They are not really living up to the spirit of law, and now, to make it even worse, we have to share—we have an obligation if they comply with the basic rubric of anti-money laundering and terrorist financing, combatting that, that we have an obligation to share information with them.

And I am wondering, is there a better way to use the name-and-shame, the Wolfsberg principles, against some of these countries that are just—I think they have been less than diligent in their effort to combat terror financing?

Mr. COMRAS. I agree with you completely. I think that much, much more has to be done to hold accountable international financial institutions, and one of the best tools to do that is naming and shaming. Between 2003 and 2008, FATF put a moratorium on naming and shaming, but thankfully, in 2008, they began that process again of indicating which countries lacked the political will

or the wherewithal to apply their financial rules in any meaningful way. I think that FATF has to continue to do that kind of an action.

I think that we have to look at groups. We have a committee of the United Nations, a group that works under this resolution 1373, called CTED, and another group that provides assistance to the Security Council with respect to al Qaeda and the Taliban. They are well placed to begin to monitor and report on what is actually occurring in this area. And I think they need to be encouraged to take that kind of action.

Mr. LYNCH. Thank you, Mr. Chairman.

I yield back.

Chairman MOORE OF KANSAS. I thank the gentleman.

The Chair next recognizes Mr. Paulsen for 5 minutes.

Mr. PAULSEN. Thank you, Mr. Chairman.

I just want to follow up with Mr. Caruso on the questioning that was just taking place regarding the SAR narratives. In your testimony, you had mentioned that writing the SAR narrative is as time-consuming as ever, and putting aside whether structuring infractions should be subject to such a requirement, how useful is the narrative portion itself for law enforcement? How useful is the narrative?

Mr. CARUSO. It is very useful when it is describing matters that are of interest to law enforcement. For a case involving significant fraud or money laundering, narcotics trafficking, perhaps terror financing, a well-written narrative will grab the attention of a law enforcement agent, and that makes the difference between a law enforcement agent starting an investigation or not.

So a SAR narrative is very important when applied to matters that require the telling of a story. Structuring rarely requires the telling of a story.

Mr. PAULSEN. Regarding the structuring SAR that you describe, is it your view that these would be composed only of objective information, and this could almost entirely be compiled by advanced software systems and filed instantaneously?

Mr. CARUSO. Largely. Obviously, there would be the opportunity for the bank to add some narrative description if they would choose to do so. But most structuring is objective. It is detailing the amounts of the transactions, the day on which they occurred and who conducted the transactions.

Mr. PAULSEN. Would there be value for law enforcement of having the capability of filing such reports in realtime?

Mr. CARUSO. Absolutely, and that is an important point. Most of the structuring SARs are filed anywhere from 30 to 60 days after the event has taken place. One of the reasons is the software systems, and also the other reason is the regulatory requirements to compile a lengthy narrative.

Mr. PAULSEN. Any other suggestions you might have about changing the SAR form?

Mr. CARUSO. No. I think my view is that the structuring work is what takes up the most amount of time, so let's look at the things that we can get the most return on in proving, and that to me would be the most important. And then I am sure there would be others after that, but that one would be first.

Mr. PAULSEN. Thank you, Mr. Chairman.

I yield back.

Chairman MOORE OF KANSAS. I thank the gentleman.

The Chair next recognizes Mr. Minnick for 5 minutes.

Mr. MINNICK. Mr. Lewis, as I think you are aware from our prior conversations, I was involved a long number of years ago in helping set up the Federal Government's response to the international drug trafficking issue. And there we found that the key to really getting at the kingpins and people who were behind drug trafficking was not opening suitcases at the Mexican border; it was following the money.

It is clear to me that things haven't changed with respect to terrorism or drug trafficking for that matter. We found that you needed a central repository that had both access and clout and interface with law enforcement, Federal, local, and international, to really make good use of information. The problem was not a shortage of information; it was analytic capability and analytic focus.

In the terrorism area, in 2005, we set up FinCEN, as Mr. Lynch was commenting earlier, to do precisely this with respect to following the money involving terrorism. Listening to the testimony of all of our witnesses, it is pretty clear to me that FinCEN has not accomplished the task. And I would like to ask you, having studied the issue, where is the deficiency at FinCEN? Is it access to information? Is it analytic capability and focus? Is it the interface with law enforcement or foreign cooperation? Where is the shortfall, and what needs to be done to fix FinCEN, so it can perform this critically important international role?

Mr. LEWIS. Thank you, Congressman Minnick.

FinCEN has probably been underresourced, and I think there is a real confusion as to whose job is what. I think there is slippage at every stage of the matter. For example, when banks do their due diligence, there is an element of "out of sight, out of mind." And when a Middle Eastern business wants to open an account in a New York bank, they are not going to have the level of communication and information that they would get if it were a New York business. That has to stop.

So there needs to be an interface between the compliance people and the business people at the bank to begin with, so that good information is coming into the United States whenever a Middle Easterner, or someone from any politically risky area of the world, wants to open an account. And they need to get that qualitative information.

They also need to have better filters so that when a business comes in, as in our case, and says, "We are going to do $15 billion of transactions," somebody there finds out why, and that is documented. And if the story doesn't add up, then that information goes to the regulators. And when that $15 billion in transactions grows to $30 billion and $35 billion, there also needs to be a red flag that goes up within the bank within the regulator.

So there is a problem of being inundated with money, but—with information—there needs to be a kind of qualitative regulation so that there is a dialogue between the regulators, the banks, and FinCEN, so everyone knows what they are looking for. I think Mr. Caruso's idea of avoiding that sea of information that is likely to

yield very little should be reconstituted so there is better qualitative dialogue between the bank regulators, who are looking to the financial safety and soundness, and FinCEN, which is really looking to the national security interests. I think everyone is stovepiped at the moment, and you don't have FinCEN having the ability to take the lead and access—

Mr. MINNICK. Does FinCEN have the access to the artificial intelligence capability to go through and sift this information and find the relevant information? There is a lot of that kind of software currently available.

Mr. LEWIS. I don't really know how their technological systems work. They certainly should.

Mr. MINNICK. They report to an Under Secretary. Is he taking his job seriously enough to provide this interface and outreach that is necessary to use the information intelligently?

Mr. LEWIS. I think the Administration does take it seriously, but there has been a failure to specify what the qualitative areas are where they really should be looking, as opposed to simply generating reams of information according to abstract categories that have no real meaning in the real fight against terrorism.

Mr. MINNICK. Thank you.

And finally, where did that trillion dollars go?

Mr. LEWIS. We don't know, and that is the big problem, because even if we could account for 99 percent of it, there is so much money unaccounted for, and it poses a real danger to our system and to the national security interests of this country.

Mr. MINNICK. Thank you.

I yield back.

Chairman MOORE OF KANSAS. Mr. Lynch, you have 1 minute to respond if you would like to respond to that.

Mr. LYNCH. I can't sit and let that go. The remarks regarding FinCEN, the Financial Crimes Enforcement Network, I have worked with them very, very closely on half a dozen countries where they have done unbelievable work. The Financial Crimes Enforcement Network, FinCEN, Jim Freis over there is doing incredible work with very limited resources.

We have expanded their responsibility. Not only do they respond to every single government agency in terms of information, every foreign government, now they have been expanded. Their responsibility has been expanded to respond to State police agencies, local police departments, and they are still doing so with the same resources they had before.

I have sponsored amendments to try to increase their funding, so they can do a better job. But those people are courageous men and women over there doing a fantastic job. And I just think members need to get over there, like I have, sit down with FinCEN and get to know what they are doing and the scope of their work, and you would be very pleased with the work they are doing. They are doing unbelievable work over at FinCEN.

God bless them over there. They need more money.

The gentleman is right. They are underresourced. Mr. Lewis is absolutely correct. And we are asking them to do much, much, much more. And while we are pushing money out to these depart-

ments that FinCEN responds to, we have not given any resources, any increased resources, to FinCEN to do their job.

So, thank you, Mr. Chairman.

Chairman MOORE OF KANSAS. Thank you, sir.

And again, thanks to our witnesses for your testimony here today. Today's hearing gave us an opportunity to review the latest trends in terrorism financing and equip our committee with new insights that we will take back to the relevant Federal agencies who are staffed with top notch men and women who rarely are recognized for their efforts but play a key role in keeping our country safe. We will discuss these issues with them.

This is not and should not be a partisan issue. We all want to make sure our government has the tools and resources it needs to best combat terrorism financing.

The Chair notes that some members may have additional questions for our witnesses which they may submit in writing. Without objection, the hearing record will remain open for 30 days for members to submit written questions to these witnesses and to place their responses in the record.

The hearing record will also remain open so that anyone named in a witness statement will have an opportunity to respond to those witnesses' comments or allegations.

Again thanks to all. And our hearing is adjourned.

[Whereupon, at 5:05 p.m., the hearing was adjourned.]

A P P E N D I X

September 28, 2010

The Honorable Walt Minnick

Chairman Moore and Ranking Member, Biggert, I commend you for holding this important hearing today and thank you for the opportunity to participate. As 9/11 illustrated with jarring clarity, disrupting the financing of global terrorism is a critically important issue central to the survival of civilized society. On this, the ninth anniversary of that tragedy, we need to examine the progress that has been made and the shortfalls in the international financial surveillance system that are yet to be addressed.

Just how vulnerable is our banking system today to being the conduit through which sophisticated global terrorist groups finance their infrastructure and procure their weapons of death and destruction? How are we doing in identifying and using financial information to disrupt related endeavors such as drug trafficking, weapons sales, sanction breaking and the money laundering incident to other large scale criminal activity? We hope—and expect—that our witnesses today will give us some of the answers.

Since September 11th 2001, the U.S. government has given the agencies in charge of protecting our national security and overseeing our financial system broad grants of authority and very substantial resources to ensure that the funders of international terror are identified and their ability to transfer the funds interrupted. The PATRIOT Act, the Intelligence Reform and Terrorism Prevention Act and the Anti-Terrorism Penalty Act all were passed overwhelmingly by a bipartisan Congress. All enhanced the U.S. Government's ability to monitor foreign financial transactions, to analyze suspicious funds flows and to share that information with appropriate law enforcement agencies and our international partners in the Global War on Terror.

However, given the pre-eminence of the U.S. dollar in international commerce, the exploding volume of funds transfers and an increasing interconnected global economy which connects electronically in real time, are we succeeding? Are the systems and institutions designed to intercept terrorists, identify international drug traffickers, monitor illicit

global weapons traders and sanction breakers, and identify other criminal activity up to the task? If not, what changes need to be made?

This committee has previously discussed the lack of oversight of massive funds flows originating in the Middle East. It has studied the inter-connectiveness of global financial centers. It has explored the threats posed by banking secrecy rules in Switzerland, the Caribbean and emerging financial centers of the Far East. It has argued the tradeoffs between maintaining privacy and disclosing threats to international security.

We are here today to learn whether U.S. Financial authorities have the tools, staffing and will to successfully perform our nation's portion of this task. To discover whether foreign governments and international financial institutions are similarly focused and effective. And to understand whether this information is being shared and effectively used to arrest and imprison drug kingpins, foil Al Qaeda and other international terrorist groups, enforce trade sanctions and identify global

criminal activity. Do we understand our vulnerabilities and are we working effectively to overcome them?

These are all questions that must be answered to assure our citizens that our government is protecting both their assets and our nation's security in an increasingly dangerous and interconnected world.

Thank you Mr. Chairman. I yield back.

David B. Caruso
Chief Executive Officer
Dominion Advisory Group
Statement before the House Financial Services Subcommittee on Oversight and Investigations
September 28, 2010

Good afternoon Chairman Moore, Ranking member Biggert, and members of the subcommittee. Thank you for the opportunity to appear before you today to discuss the vulnerabilities of our financial system to terrorists and money launderers.

Financial institutions, particularly depository institutions, play a crucial role in identifying and reporting potential terrorist financing and money laundering. Over the last 10 years banks have spent considerable amounts of money to hire staff and implement software systems to detect suspicious activity. As a result, most financial institutions comply with the Bank Secrecy Act or BSA. However compliance with regulations and identifying potential terrorist financing and money laundering are not necessarily synonymous.

Suspicious Activity Reports or SARs reporting activity related to BSA violations account for nearly half of all SAR filings. The majority of these SARs are made up of those reporting attempts to evade the Currency Transaction Reporting threshold - a practice known as "structuring."

The burden of detecting, investigating and reporting cash structuring using today's version of the SAR, hampers a financial institution's ability to identify transactions associated with more serious crimes, and makes our financial system more vulnerable to terrorist financing and money laundering.

Consideration should be given to creating a new SAR designed to report only cash structuring. Such a SAR would still provide the government with needed information and would reduce the time and effort needed by institutions to complete the form, thus enabling more energy to be directed at uncovering terrorist financing and significant money laundering.

Now when institutions detect structuring they must adhere to the requirements of the Federal Financial Institutions Examination Council and FinCEN that mandate SARs include a thorough and complete narrative, or written depiction of the events that lead to the conclusion a SAR must be filed. In addition, institutions are expected to compile supporting case information into a comprehensive file. This information is used by auditors and examiners as a way to test a bank's compliance with the BSA. Over the past five years the expectations of regulators and industry practice has expanded. Writing the SAR narrative is as time consuming as ever.

A modified SAR to report structuring will still convey the relevant facts of an investigation – who, what, where, when and how much – but can be compiled into a much more concise format such as a table or spreadsheet that will inform law enforcement of what it needs to know, provide regulators with evidence of an institution's compliance with the BSA and then free up the resources of a bank to focus on detecting terrorist financing and more sophisticated money laundering schemes.

Financial institutions struggle with how to effectively detect terrorist financing. Retrospective analysis of terrorist funding does not provide clear enough

direction to bank investigators on what specific transactions may indicate funds are being sent to support terrorists. Sophisticated money launderers are as well schooled as most compliance officers in the BSA and AML regulatory requirements and they know how to skirt typical controls. Policy makers, regulators and the industry know that detecting and thwarting these types of activities is the primary objective of the BSA.

Depository institutions and other financial institutions including money service business have implemented automated software systems designed to more effectively and quickly identify suspicious activity. However, these software systems produce large numbers of alerts, mostly related to structuring, because structuring is the easiest type of activity for these systems to identify.

Satisfying the regulatory requirements around investigating, documenting, and reporting structuring takes a typical bank investigator between three (3) to eight (8) hours.

Our experience working with small, mid-sized and large banks show us that structuring accounts for between 60 – 70% of all BSA related SARs. We also see that over half of the customers that structure have neither structured before nor subsequently to the incident in question. These "one time structurers" however eat away at the time a bank's staff can then spend uncovering and investigating activity whose impact to the financial system and national security could be more serious.

Structuring SARs provide the government with important information, including information that may lead to the discovery of serious criminal activity. The importance of this information should not be minimized. What should be minimized however is the time and effort needed to report that activity. By creating a SAR tailored to report only structuring, the government would relieve financial institutions of their largest BSA/AML compliance burden and then enable institutions to use that available time and those resources to identify and report more serious crime.

Thank you again for the opportunity to testify here today.

Written Statement
Victor D. Comras, Esq
Concerning
Current and Evolving Trends in Terrorism Financing
before the
Subcommittee on Oversight and Investigations
Committee On Financial Services
U.S. House of Representatives
Washington DC
September 28, 2010

Mr. Chairman,
Distinguished Members:

Thank you for inviting me here today to express my views and concerns with regard to US and international efforts to stem the flow of financial support to terrorist organizations.

We have just passed the 9th Anniversary of the terrible 9/11 attack that confirmed for us, and for most of the international community, that international terrorism poses one of the gravest threats to international peace and security. Yet, despite this confirmation, funds continue to flow to those engaged in indoctrinating, recruiting, and training terrorists and for terrorist operations.

Some have suggested that we have, in fact, already put a real crimp on terrorist financing. But, the threat posed by the international terrorists has not diminished. And, empirical evidence demonstrates that many of these terrorist groups, including al Qaeda, the Taliban, Hamas, Hezbollah, Lashkar-e-Taiba, and other groups associated with al Qaeda, continue to have access to sufficient funds to maintain their organizations and their terrorist operations. If anything, Taliban funding is expanding, not diminishing.

While the Taliban's cash flow from Afghanistan's poppy fields comes as no surprise, the amount of foreign donations they continue to receive is a real eye opener. According to the CIA (as reported in the Washington Post), Taliban leaders and their allies received some $106 million in the past year from donors outside Afghanistan. Much of these funds are drawn from the same donors in Pakistan, the Gulf region, Southeast Asia and Europe that long supported al Qaeda. And these supporters continue to include a variety of Muslim fundamentalist organizations and charities, as well as wealthy Al Qaeda/Taliban supporters.

Hamas has also developed its own worldwide network for soliciting funds to support its activities, including terrorism-related operations. Hamas, which has close links with the Muslim Brotherhood, is also still able to use front companies and well-established banking links in much of the world to openly collect such funds from organizations, donors, and from over the internet, and to transfer these collected funds to Hamas operatives through well established channels.

There is also a growing nexus between terrorism and transnational crime. The Taliban, FARC and several other international terrorist groups draw heavily on funds generated from the illicit drug trade and other criminal activities, including petty crime and credit card fraud, and even Hamas has turned to the illicit drug trade emanating from the tri-border region in Latin America to surreptitiously acquire additional funding. West Africa and Southeast Asia are also emerging as other potential regions for this crime-terrorism convergence.[1] And these nexus rely heavily on money laundering techniques to enter these funds into established financial transfer channels.

I know, Mr. Chairman, that U.S. financial institutions take the threat of international terrorism very seriously. They have come a long way since 9/11 in

[1] See CRS Report "International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress, March 18, 2010 prepared by John Rollins and Liana Sun Wyler

putting in place effective procedures to identify, report, and/or to block suspicious transactions. Extensive transaction filters have been put in place and "due diligence" and "know your customer" have become regular catchwords for compliance officers spread extensively throughout our banking and financial system. And, US Government regulatory oversight is now both intensive and vigilant.

So, what is lacking?

Well, Mr. Chairman, the fact is that US Banks are intricately networked into an international banking system that has not yet fully come to terms with halting terrorism financing. And, while we have made great strides in cutting off the flow of money for terrorism from the United States, our banks remain awkwardly vulnerable to getting caught up in handling terrorist group-related transactions that originate overseas. This is because US banks must so heavily rely on the veracity and accuracy of the transactional information provided to them by their overseas clients and associates.

Following enactment of the increased "due diligence" and "know your customers" requirements contained in the Patriot Act, US banks moved quickly to re-assess their relationships with the foreign banks with whom they maintain a correspondent relationship. They had to assure themselves that these foreign banks were also taking the steps necessary to vet their clients and that they would accurately record and pass on required transactional information, including the correct identification of the beneficial parties involved. But, the fact is that this is not always the case. And, in the fast and very competitive world of international financial transactions, these assurances are often shortchanged. Our banks must also rely heavily, therefore, on any cautionary information that our public sector regulatory agencies, such as Fincen, OFAC, and other relevant Treasury Department offices share with them. This cooperative relationship and information sharing is essential, and needs to be formalized.

Today, when US banks have doubts about the legitimacy of transactions they are required to file suspicious activity reports with FinCen. In most cases they still permit the transaction to be processed. However, when their doubts suggest the possibility of terrorism financing, they will usually place some kind of hold on the transaction.

US Depository Institutions filed some 15,500 suspicious wire transfer reports in 2009. Of these, only about 545 involved possible terrorism financing concerns. How well they are actually doing in discerning such terrorist-related risks remains any ones guess. Nevertheless, the number of suspicion-of-terrorism SARS did increase some 8 percent last year.

Considerable strides have also been made with regard to the regulation and oversight of the myriad money services businesses operating in the United States. This sector has seen exponential growth in the volume of international financial transfers. We must recognize, however, that at least one part of this sector – the informal mom and pop transfer mechanisms, such as Hawala, lack the wherewithal to closely vet the transactions they handle and they remain particularly vulnerable to being used to handle terrorism related transfers. Here too, much of the problem resides overseas. Funds transferred through Hawala like systems are very hard to trace, particularly as they are re-directed once they are received overseas. Terrorist organizations have become sufficiently sophisticated in handling such transactions to assure that the initial overseas recipient of the funds appears squeaky clean.

Let me suggest, Mr. Chairman, that it is essential that we broaden the focus of our attention, when it comes to inhibiting the financing of terrorism, to include financial institutions beyond our shores.

When I say that the locus of the terrorism financing problem is largely overseas I do so with a caveat. A number of foreign financial institutions that maintain branches and correspondent accounts in the United States have engaged in banking activities that have become of grave concern to us.

In August 2005, the New York branch of Jordan's Arab Bank signed a consent decree, and paid a $24 million penalty, for its involvement in transferring more than $20 million to and from more than 45 suspected terrorists or terrorist groups in the Middle East. The bank acknowledged that it had dollarized many of these transactions. In April 2009, Doha Bank, New York paid a civil penalty of $5,000,000 which was assessed, in part, because of its involvement in dollarizing transactions related to terrorist groups overseas.

There have been several other cases involving US branches of foreign banks that have engaged in practices inconsistent with U.S sanctions laws and regulations. Last May a criminal information was filed against, ABN AMRO, now part of the Royal Bank of Scotland, for facilitating transactions by altering or stripping information from the transactions so that they might pass undetected through compliance filters at other U.S. financial institutions. These transactions involved more than $3.2 billion dollars moving to, from, and through AMB AMRO's New York branch. And, in December 2009, Credit Suisse was assessed a $536 million penalty for processing thousands of transactions over a 20-year period that concealed the involvement of sanctioned parties and the routing of wire transfers and securities transactions to and through the United States.

These regulatory actions have sent a strong message to overseas financial institutions that the United States will not countenance such activities on the part of their branches in the United States.

But, an even stronger message is now being sent by victims of terrorism as they move in U.S. courts to hold such financial institutions accountable under section

2333 of the anti terrorism act for facilitating the flow of funds to terrorist organizations. I cite as examples the civil damages cases now proceeding in New York against Arab Bank, Nat West, and Credit Lyonnais for their having facilitated the transfer of funds to Hamas and other terrorist groups that have launched suicide and other terrorism attacks against innocent victims in Israel.

The real problem here is that while these terrorist related transactions are illegal in the United States, they have not been deemed illegal by many of the other countries in which these banks operate. This is in spite of the fact that almost all countries are now parties to the International Convention for the Suppression of the Financing of Terrorism, which came into force in April 2002. That convention clearly obligates all countries to criminalize the funding of groups or individuals that engage in terrorist activities.

Shortly after the 9/11 attack the Security Council also adopted resolution 1373 which obligates all countries, whether or not they have adopted the Terrorism Financing Convention, to take the steps necessary to prevent the transfer of funds to terrorist organizations or for terrorist purposes. But, the resolution failed to contain any definition or criteria as to what constitutes terrorism. It left it to each country, independently, to determine this crucial issue for itself. Without common criteria, or a definition of terrorism, each country remains free to interpret its own obligations. Each can decide which groups they consider terrorists and which they wish to hail as "freedom fighters." Saudi Arabia uses this distinction, for example, to justify its continuing funding for Hamas while Iran and Syria use it to provide funds and support to Hezbollah.

The fact of the matter is that there is still only a very limited international consensus as to which organizations are terrorist organizations. And, for the most part, that consensus is limited to a very short list of entities and individuals identified and designated by a Committee of the Security Council, as being directly associated with al Qaeda and/or the Taliban.

At my own last count, in June 2010, that designation list includes 137 members of the Taliban, 257 members or associates of al Qaeda, and 103 entities directly related to al Qaeda. I want to be clear on this point. Beyond that list of designated individuals and entities there is no international consensus, and therefore, no clear and enforceable international obligation, which inhibits countries from allowing their financial institutions to engage in financial transactions with such undesignated individuals and entities.

Only a limited number of countries have joined with us in designating such organizations as Hamas and Hezbollah as terrorist organizations. This includes, for the most part, our European friends and allies. Yet, some European countries still exempt the political and humanitarian wings of these organizations from such designation. Many other countries have not even gone that far and openly permit their financial institutions to process transactions in Hamas' and Hezbollah's favor.

Given US bank interaction with this larger international banking community, the vulnerabilities become stark. And, that means that very careful attention must be paid to assuring that accurate information regarding origination and the ultimate recipient of the transaction is complete and accurate.

The problem is further complicated by the emergence in numerous lesser developed countries of new under-funded and under-regulated home grown banks. These banks rely heavily on their correspondent and payable through accounts maintained in more established banking institutions. Many of these home grown banking institutions continue to lack the wherewithal to mount and maintain an effective compliance system. At the same time the national regulatory environment under which they operate is unable to provide effective oversight. And, many of these banks are located in areas quite susceptible to the recruitment of terrorists.

So, Mr. Chairman, I would also place great emphasis on the need to strengthen the international banking communities resources and commitment to halting the financing of terrorism.

I do not want to appear too pessimistic in this regard. A very substantial segment of the international banking community does take terrorism financing and money laundering issues quite seriously. The Wolfsberg group of banks, for example, has established high standards to prevent terrorist organizations from accessing their financial services, and they have pledged to assist governments in their efforts to combat terrorist financing.

There are also a number of other activities underway to upgrade international compliance capability. FATF, The Financial Action Task Force, has made great strides in providing guidance and best practices for the strengthening of international banking compliance, and in brokering assistance for jurisdictions wishing to upgrade their compliance programs. It has also spawned numerous regional organizations to facilitate cooperation and share the burden of compliance among their member banks.

FATF has also finally gotten back to holding certain countries accountable for their failings in this regard. In 2008 FATF began publishing a list of high risk and non cooperating jurisdictions whose banks have failed to adequately implement an anti-money laundering and counter terrorism financing program. FATF issued a series of statements expressing concerns about the AML/CFT deficiencies in Iran, Uzbekistan, Pakistan, Turkmenistan, São Tomé and Principe, and the northern part of Cyprus.

The FATF statements called on FATF members to pay special attention to transactions dealing with Iran and Uzbekistan and to strengthen preventive measures in response to the risks associated with these countries. In February

2009, FATF also called on its members and other jurisdictions to apply additional counter-measures to protect their financial sectors from money laundering and terrorist financing risks emanating from Iran.

Ultimately, United States regulatory agencies can also make reference to the broad powers provided to them in Section 311 of the Patriot Act. As you know, Mr. Chairman, that section authorizes the Secretary of the Treasury to impose special enhanced due diligence requirements with regard to the maintenance and operation of correspondent and payable through accounts maintained in US banks for foreign jurisdiction banks. And, in some cases this may include precluding the operation of such accounts in favor of risky banks overseas.

We all recognize that these powers must be used sparingly and prudently. At the same time they do provide us considerable leverage when it comes to influencing and correcting bad banking conduct overseas.

Thank you, Mr. Chairman.

FLAWED DIPLOMACY

THE UNITED NATIONS & THE WAR ON TERRORISM

VICTOR D. COMRAS

Potomac Books

FOR IMMEDIATE RELEASE

CONTACT: Claire Noble
Tel: 703-996-1017
E-mail: Claire@booksintl.com
www.potomacbooksinc.com

"A courageous attempt to lift the veil of secrecy over the many failures of the war on terror."

FLAWED DIPLOMACY

The United Nations & the War on Terrorism

There have been numerous attempts to engage the United Nations in a meaningful campaign against state-supported and other terrorist activities. But the inherently political nature of terrorism has made it exceedingly difficult to gain global consensus on who even qualifies as a terrorist, much less agreement on counterterrorism measures to pursue.

The rise of al Qaeda, the events of 9/11, the Madrid train bombing, and the London mass transit bombings provided the international community and United Nations with new impetus to respond to terrorism. A series of Security Council resolutions and international conventions were adopted outlawing terrorism while the UN fruitlessly sought to identify and address terrorism's root causes. Yet, terrorist groups prospered and the threat posed to international peace and security intensified. The UN now stands at a crossroads that will determine whether the international community can move in concert against terrorism, or must leave that task to the piecemeal approach adopted by key nations as they act separately to preserve their own homeland security

As one of five Security Council–appointed international monitors on the measures being taken against al Qaeda and the Taliban, Victor D. Comras had the rare opportunity to observe the UN's counterterrorism activities. He delves into the organization's role in dealing with terrorism, explores the international political realities and institutional problems that make it difficult for the UN to successfully implement and monitor counterterrorism measures, and describes both its successes and failures, ultimately laying out a case for creating a stronger, more effective UN response. *Flawed Diplomacy* is an invaluable resource for anyone interested in the war on terrorism and in gaining knowledge about the UN's inner workings.

Victor D. Comras is a leading expert on international sanctions and the global effort to combat terrorism and money laundering. A seasoned U.S. career diplomat, Comras frequently testifies before Congress on these issues and is a regular commentator on radio and television. His articles have appeared in numerous online journals and in the *Washington Post*, the *Financial Times*, and other publications. He is also a contributor to *Terrorism Financing and State Responses: A Comparative Perspective* (2007). He resides in Ft. Lauderdale, Florida.

The author is available for interviews. If interested, please contact Claire Noble at 703-996-1017 or Claire@booksintl.com.

Flawed Diplomacy: The United Nations & the War on Terrorism
Victor D. Comras
October 2010, Cloth, 978-1-59797-438-7, $29.95, 256 pp, 6 x 9

Published by Potomac Books, Inc.
22841 Quicksilver Drive, Sterling VA 20166

Tel: 703.996.1017
Fax: 703.661.1547
www.potomacbooksinc.com

Potomac Books

FOR IMMEDIATE RELEASE

CONTACT: Claire Noble
Tel: 703-996-1017
E-mail: Claire@booksintl.com
www.potomacbooksinc.com

Flawed Diplomacy continued

About the Author

Victor D. Comras

Victor D. Comras is a leading expert on international sanctions and the global effort to combat terrorism. A seasoned career diplomat of the United States, he was chosen by UN Secretary-General Kofi Annan to serve as one of five international monitors overseeing the implementation of Security Council measures against terrorism (al Qaeda) and terrorism financing. During its short two-and-a-half-year tenure, this controversial group pinpointed many of the most serious problems and deficiencies in the international application of counter-terrorism measures. Comras frequently testifies before Congress on these issues and is a regular commentator on radio and television.

Published by Potomac Books, Inc.
22841 Quicksilver Drive, Sterling VA 20166

Tel: 703.996.1017
Fax: 703.661.1547
www.potomacbooksinc.com

Potomac Books

FOR IMMEDIATE RELEASE

CONTACT: Claire Noble
Tel: 703-996-1017
E-mail: Claire@booksintl.com
www.potomacbooksinc.com

Flawed Diplomacy continued

Advance Praise

"*Flawed Diplomacy* is a courageous attempt to lift the veil of secrecy over the many failures of the war on terror. Comras, a lawyer and a veteran of the anti-terrorism struggle, shows with amazing clarity how the United Nations efforts to bring to justice Osama bin Laden and his inner circle of followers did not succeed. On the background of this compelling tale of lost opportunities we find the crumbling of the fragile political equilibrium of key Muslim states: from Iraq to Afghanistan. A must read for those who want to understand what really happened inside the UN during those key years of the war on terror."
Loretta Napoleoni, economist and author of *Terror Incorporated* and *Terrorism and the Economy*

"A counterterrorist practitioner, Victor Comras contributed appreciably to dismantling the terrorist support infrastructures. In *Flawed Diplomacy*, Comras chronicles the challenges and opportunities involved in creating a global counterterrorist environment."
Rohan Gunaratna, author of *Inside Al Qaeda* and co-author of *The Terrorist Threat from Thailand*

"*Flawed Diplomacy* is a meticulously crafted account of a protracted struggle between the nation-state system and the forces bent upon its destruction.
Comras lays out this struggle in precise, dispassionate detail. Depending on whether or not we heed the lessons of recent history, Flawed Diplomacy has the potential to serve as part of the narrative of a successful escape from a close call with disaster.
If, on the other hand, these lessons are ignored, Comras's book could come to be seen as the first chapter in the tragic history of our collective failure to counter the terrorist threat."
Leon Fuerth, Research Professor of International Affairs, Elliott School of International Affairs, The George Washington University, and former national security adviser to Vice President Al Gore

"*Flawed Diplomacy* is an essential read for those who wonder where counterterrorism policy has gone astray. In a firsthand account that is devoid of ego but substantial on case knowledge and policy options, Vic Comras discusses the successes of UN counterterrorism policy and its failures due to big power politics, lack of institutional capacity, and shortness of vision. As we approach the tenth anniversary of 9/11, Comras clearly lays out the work that remains to be done to build a successful multilateral policy against al Qaeda."
George A. Lopez, professor of peace studies, University of Notre Dame

Published by Potomac Books, Inc.
22841 Quicksilver Drive, Sterling VA 20166

Tel: 703.996.1017
Fax: 703.661.1547
www.potomacbooksinc.com

FOR IMMEDIATE RELEASE

CONTACT: Claire Noble
Tel: 703-996-1017
E-mail: Claire@booksintl.com
www.potomacbooksinc.com

Flawed Diplomacy continued

Sample Interview Questions and Discussion Points

- What role can the United Nations (UN) effectively play in combating terrorism?
- What tools can the UN put into place to deal with terrorism? Do these tools really work?
- What can be done to improve the UN's role in combating terrorism?
- Why has the UN failed so miserably when it comes to dealing with terrorism in the Middle East?
- In your opinion, do you think the UN Security Council should act more vigorously when it comes to the issue of Palestinian terrorism?
- Do you think that the UN frequently blames Israel and overlooks terrorism in Palestine?
- What has the UN done to address the root causes of terrorism?
- What is the UN doing to deal with Al Qaeda and the Taliban?
- What has the UN done to curtail terrorist financing?
- Is the UN doing anything to stop terrorists from acquiring weapons of mass destruction?
- Why is a comprehensive definition of terrorism important?
- After more than a decade of trying, why has the UN been unable to agree on a definition of terrorism?
- Are we sacrificing human rights to the war on terror?
- Why doesn't the UN do more to assist the victims of terrorism?
- What's involved in the UN designation of terrorists? Doesn't that process violate due process?

Published by Potomac Books, Inc.
22841 Quicksilver Drive, Sterling VA 20166

Tel: 703.996.1017
Fax: 703.661.1547
www.potomacbooksinc.com

Flawed Diplomacy: The United Nations & The War on Terrorism

By
Victor D. Comras

Book Excerpts

The following are excerpts intended to provide potential readers a sense of the book's content and thesis. They have been arranged in a manner to serve this purpose.

On the Role of the United Nations

"The United Nations is considered by many as the essential organization in international affairs. It is the central forum where the international community comes together to interact and to provide the political, moral and legal basis for international action. The organization's principal mission has always been to work for, and preserve, international peace and security, and its Charter provides a broad mandate for UN action. Yet, when it comes to terrorism, perhaps today's gravest threat to international peace and security, it has been hesitant, slow to act, and less than effective."

****

"There were numerous attempts over the years to engage the United Nations in a meaningful campaign against State supported and other terrorist activities. But, on each occasion, the issues were hijacked by the defenders of those groups engaging in terrorism. They were deemed "insurgent groups" or "freedom fighters" and defended on the basis that they were really asserting, or fighting for, "self determination," or otherwise engaged in popular uprisings or "civil wars." This made it exceedingly difficult to gain an international consensus on these issues. This "lack of consensus" resulted, and continues to result, in many countries justifying their continuing support for such groups as Hamas and Hezbollah, despite their evident use of terrorist tactics to achieve their objectives."

****

"The United Nations, itself, is ill-suited for taking on an enhanced sanctions enforcement role beyond monitoring, observing and reporting on compliance issues. UN procedures are cumbersome and very political. Diplomatic niceties and political realities hamper timely and forthright action. And few countries have been willing to share sensitive information or intelligence on terrorism to so broad a forum. The UN Secretariat has little grounding in counter-terrorism expertise. And secretariat hiring procedures may not be conducive to putting together the needed secure expert human resource base. During the Bosnian war, for example, the UN had to be convinced to turn over implementation to regional enforcement groups in order to get the sanctions on Serbia to work. These sanctions then became the most successful in United Nation's history."

On airline hijackings and the road to 9/11

"The road to 9/11 might well be said to have begun with the hijacking of El Al flight 426 from London via Rome to Tel Aviv on July 23, 1968. Three well dressed Arab passengers, carrying concealed pistols and hand grenades, commandeered the plane in flight. They ordered the plane's captain, Oded Arbarbanell, to head for Algiers....The Israeli government, which had no relations with the Algerian government, appealed directly to the UN Security Council, the ICAO, and other international air transport organizations for assistance in obtaining the release of the plane, passengers and crew, but to no avail.... While the Security Council debated, and the ICAO made references to article 11 of the 1963 treaty, not yet in force, Israel was forced, on its own, to seek out a friendly intermediary through which it might engage in some form of negotiations with the hijackers. After five long weeks of stalemate, Israel agreed to hand over 16 convicted Arab terrorists, in exchange for the Israelis' safe release, establishing blackmail as a precedent that would long haunt the international community. No punitive action was ever taken against any of the hijackers."

On the UN's failure to respond to the Munich Olympics Terrorist Attack

"The terrorist attack at the Munich Olympics had sparked international outrage, and Waldheim knew that the credibility of the United Nations was on the line. But, he failed to anticipate the strong opposition he would encounter from the General Assembly's G77 and Non Aligned Movement members. Nor did he envisage that Western European countries initially behind his initiative would go soft so quickly. Despite the international outcry, not one UN member had put the Munich terrorist attack on the Security Council's or General Assembly's Agenda. The Waldheim counter-terrorism initiative turned out to be a complete fiasco, and set a tone of debate that stymied the General Assembly's ability to move forward productively against terrorism for the next two decades. If anything, the exercise underscored the rift that had developed between third world's developing countries and the West. And, the Soviet Bloc showed itself eager to exploit this growing rift."

On the UN's response to 9/11

"The United States and the other authors of the resolution ...hoped that resolution 1373 {adopted shortly after 9/11} and the Counter-Terrorism Committee it established, would provide a useful platform for exchanging intelligence and other information on terrorists, their plans, support mechanisms and capabilities.... {But} without common criteria, or a definition of terrorism each country remained free .... to decide for themselves which groups should be called terrorists and which were to be hailed as "freedom fighters." Saudi Arabia used this distinction, for example, to justify its continuing funding for Hamas while Iran and Syria used it to provide funds and support to Hezbollah. Many other countries also simply avoided taking any steps to freeze funds or take other civil or criminal action against those individuals or groups whose political goals they supported."

****

"Convincing the Security Council to adopt a system that would lead to the identification of specific individuals and entities as terrorists, and require each country

to take action to freeze their assets, deny them access to economic resources, stop their travel, and impose an arms embargo against them, posed a much greater challenge. ... The designation system contained in resolutions 1333 and 1390.... was highly controversial and had already come in for heavy international criticism. It is no slight accomplishment that the United States was still able to negotiate such an arrangement and to get the other 14 Security Council members to sign on. This was the first time that the Security Council was willing to specifically name, and act against, any terrorist organization."

On post 9/11 actions and failings

There can be no doubt that the international community, with help and direction from the UN Security Council, and its various counter-terrorism activities, has made strides in countering and stalemating al Qaeda and the Taliban. In the eight years since the 9/11 attacks Al Qaeda and its associated networks have lost considerable strength, both structurally and in the forum of world public opinion, Yet, both Al Qaeda and the Taliban remain undefeated and resurgent. And, they continue to pose, in the words of a recent U.S. State Department report, "the greatest terrorist threat" to international peace and security. Having found refuge and safe haven in the remote Pakistan/Afghan border area and in Pakistan's Federally Administered Tribal Areas (FATA), they have worked to reconstitute themselves, and have re-established and expanded upon links and lines of influence with disparate sympathy groups around the world willing to do their bidding"

****

"The contemporaneous terrorist attacks and bombings in Saudi Arabia, Chechnya, Morocco and Afghanistan stood as strong witness to the fact that al Qaeda and like-minded groups continued to pose a significant threat to international peace and security. The war in Iraq and its aftermath had also become recruitment posters for al Qaeda around the world. The Committee's Consolidated List was not keeping pace with the changes occurring in Al Qaeda's structure or leadership, and increasingly became outdated. It increasingly became apparent that al Qaeda had been able to reconstitute a significant, even if somewhat smaller, financial support network. This network relied heavily on charities, the internet and informal transfer mechanisms. Curtailing al Qaeda's access to these financial resources would require a sustained international cooperative effort. Yet, implementation and enforcement of the asset freeze and other sanctions measures remained uncertain, uneven and lagging; nor had there been improvement in the sharing of information between countries facing the threat of al Qaeda terrorism."

****

"On September 14, 2005, world leaders from some 150 countries came to New York for a three-day United Nations Summit. The event also marked the opening of the General Assembly's sixtieth anniversary session. International terrorism was one of the key issues to be addressed. And once again, loud condemnations of international terrorism and calls to action were voiced by just about each speaker. President George Bush was among the first. Terrorism, he reminded the chamber, had come to Tunisia, to Indonesia, to Kenya, to Tanzania, to Morocco, to Israel, to Saudi Arabia, to the United States, to Turkey, to Spain, to Russia, to Egypt, to Iraq and to the United Kingdom. And those who have not seen attacks on their own soil still shared in the sorrow -- from Australians killed in Bali to Italians killed in Egypt, to the citizens of dozens of nations who were killed on 11 September 2001. 'The

terrorists must know,' he said. 'that the world stands united against them. We must complete the comprehensive convention on international terrorism that will put every nation on record. The targeting and deliberate killing by terrorists of civilians and non-combatants cannot be justified or legitimized by any cause or grievance."

On the role of the Security Council

"The Security Council has now spent the last nine years talking to itself about the need to upgrade international compliance with the counter-terrorism norms that have been put in place. And, its recent counter-terrorism resolutions have stressed the importance of compliance, and call on countries and its own committee's to do more in this regard. Yet, UN monitoring activities remain very discrete, "naming and shaming" is shunned, and, since 9/11 no country has been held accountable for its counter-terrorism failings. Little, if any, use has been made of the thirteen international conventions now in place for dealing with terrorism. And, apart from the special circumstance situations of Libya, Sudan, and the Taliban, the Security Council has failed to threaten or take action against any country for failing to comply with international counterterrorism norms."

On implementation of Security Council measures and "naming and shaming"

"Effective monitoring and oversight are critical for effective international sanctions. For international sanctions to work there must be some assurance that the measures are being applied equally and effectively by all the key players. If not, the sanctions are easily circumvented and undermined. While the UN Security Council is well placed to design and impose sanctions, and can draw on necessary expertise for this purpose, it is not well placed to oversee and monitor actual implementation and enforcement of the sanctions. That function must be assigned to an independent group which, in turn, can make its findings known to the Security Council. Such an independent group would bring increased transparency and credibility to the sanctions enforcement process. It would also place increased pressure on countries to comply with the sanctions measures. The al Qaeda and Taliban Sanctions Committee and the Security Council itself, will never be in a position to truly question what specific countries are doing in this regard. There is just too much diplomatic and political baggage involved in their initiating such inquiries or findings, except, perhaps for the most egregious cases which might themselves merit special Security Council action."

****

"Government officials were always willing to present their own standard "dog and pony show," and to reiterate the self serving points contained in their submissions to the Al Qaeda Committee, but they were uniformly reticent to share real details or sensitive information with members of the Monitoring Group. Many governments also interposed investigational, judicial or banking secrecy restrictions with regard's to the Group's inquiries. To compensate, the members of the Monitoring Group made private contact with counter-terrorism investigators and researchers, former intelligence officers, and experts at universities and in the private sector. Several members of the team also reached out to former government colleagues for potential information links and assistance."

****

"During a press conference associated with the presentation of the July, 2003 report to the Committee, the chairman of the Group, Michael Chandler, was asked whether the report would indicate links between the Saddam Hussein regime and al Qaeda. Chandler responded that "nothing has come to our notice that would indicate links. That doesn't mean to say it doesn't exist. But from what we've seen the answer is no." This simple, frank and honest response immediately captured broad media attention. For, this response seemed to contradict one of the factors claimed by the United States as justification for taking military action against Iraq. Mr. Chandler's response provoked anger and an immediate response from senior members of the Bush Administration. Small minds in Washington, and perhaps at the U.S. Mission in New York, as well, began to question US interest in maintaining its support for an independent Monitoring Group. It appeared that from that moment the Monitoring Group's days were numbered."

****

"The Monitoring Group's mandate was unceremoniously allowed to expire on January 17, 2004. And, on January 30th the Security Council adopted resolution 1526 – a resolution that tried to go in two directions at the same time. Security Council members recognized on the one hand that something had to be done to stimulate broader and more effective implementation of the measures it had adopted against Al Qaeda and the Taliban. This required additional encouragement and pressure on countries to comply. On the other hand, Security Council members no longer favored the close oversight and "naming and shaming' approach adopted by the Monitoring Group. The solution appeared to some, at the time, to transfer the role that had been played by the Monitoring Group to the Al Qaeda and Taliban Sanctions Committee itself. The Committee could then draw on expertise to be provided by a new panel under its tight control.

****

"Those in charge in Washington may have believed that by transferring the oversight responsibility directly to the al Qaeda and Taliban Sanctions Committee itself, they would somehow strengthen sanctions enforcement. But, this was a big mistake. And, the U.S. Delegation made a serious error in judgment supporting this new arrangement. It should have been clear to seasoned American diplomats that such a move would be deleterious to sanctions implementation and counterproductive to holding countries accountable, which were primary U.S. diplomatic objectives. How could they not have understood that the Security Council is, inevitably, an extremely political body. Its actions and decisions are always governed by diplomatic and political factors. Such factors would clearly constrain the Committee from holding specific countries publicly accountable, even in the most egregious situations. And, with the demise of the Monitoring Group, the U.N.'s ability to hold countries accountable was, in fact, seriously diminished."

On the role of the General Assembly

"There can be no doubt that the General Assembly has come a long way since its failure to respond positively to {the Munich Olympic terrorist attack}. The international community is long passed the period when a majority of UN members are more interested in castigating the West for colonialism then they are in coming to grips with the significant threat posed by international terrorism. However, the General Assembly continues to remain a chamber of words rather than deeds. And, to that extent, the real value of its deliberations has been to demonstrate that the

international community is fed up with the threats, horror and tragedy of the senseless violence associated with terrorism. It has reached the point when it is no longer willing to seek to justify such actions, except, perhaps, when the terrorist violence is directed against Israel. Too many countries in the Middle East and elsewhere continue to justify, motivate, support and employ groups that use terrorist tactics in the furtherance of their goals. It is this continuing hypocrisy that has deprived the General Assembly of the full force of its moral strength in dealing with terrorism."

On the role of UN Secretary General

"UN Secretary Generals are viewed internationally as the face and voice of the United Nations, and generally enjoy great public prestige and influence. They also effectively set a tone of work for the vast secretariat over which they ostensibly have some control. Some have used the position as a bully pulpit, while others have been more reserved in their presentations and pronouncements. While some clearly recognized the threat that terrorism posed to international peace and security, they were all, but one, reluctant to deviate from the low key posture on this issue adopted in both the Security Council and the General Assembly. And, when called upon to play some role, they preferred to treat terrorism within the context of the broader political situation. Of course, terrorism was then still viewed mostly as an extension of local insurgencies, or as a State backed covert activity. Kofi Annan would be the first Secretary General to break away from these constraints and to seek to play a greater role in designing and influencing international strategy for combating terrorism."

****

"The real measure of success will come when the Secretary General can report, not only on UN agency activities, but also on concrete results, such as adoption of a comprehensive counter-terrorism convention and a consensus definition of terrorism, information on steps actually taken to implement counter-terrorism laws and measures, reports on assets frozen, improvements in border controls or in safeguarding weapons of mass destruction, and statistical improvements in the number and intensity of terrorist attacks,. These elements still appear to be lacking in the Secretary General's progress reports."

A REVIEW OF CURRENT AND EVOLVING TRENDS IN TERRORISM FINANCING

Written Testimony Submitted to the House Committee on Financial Services, Subcommittee on Oversight and Investigations

Tuesday, September 28, 2010

Stephen I. Landman
Director, National Security Law and Policy
The Investigative Project on Terrorism

Chairman Moore, Ranking Member Biggert, and distinguished Members of the Committee: thank you for holding today's hearing for "A Review of Current and Evolving Trends in Terrorism Financing." My name is Stephen I. Landman, and I am the Director of National Security Law and Policy at the Investigative Project on Terrorism (IPT). I am honored to speak before you today, and hope that the work we have done at the IPT will be useful as this committee looks to combat the evolving threat of terrorist financing.

In the past decade, the speed with which the United States has developed, implemented, and fine-tuned a national counter-terrorist financing strategy has been nothing if not impressive. To date, the government has convicted over 420 terrorism suspects, with many of these cases relying upon evidence of terrorist financing. Financially, terrorist groups from al Qaida in the Arabian Peninsula (AQAP) to Hamas in the Gaza Strip and al-Shabaab in Somalia are on the ropes. By one account, al Qaida is in the "worst financial shape it has been in years."[1]

Despite these successes, much work remains to be done. Foreign Terrorist Organizations (FTOs)[2] continue to raise and move money for the purposes of recruitment, indoctrination, logistical support, training, and for their murderous acts. In part, this is due to the fact that terrorist financing—the provision of something of value to persons or groups engaged in terrorist activity—is exceedingly difficult to track. Like the terrorist groups themselves, terrorist financing crosses both geographic borders and technological boundaries.

The topic of today's hearing is monumentally important. In the ongoing effort to combat terrorism, the ability to keep money out of the coffers of these groups not only means the difference between a group undertaking an attack or not, but may have an impact on the long-term viability of the organization. Effectively responding to this threat requires a two-pronged approach: (i) understanding the means by which terrorist organizations raise money, and (ii) identifying the methods by which they move money around the globe to fund acts of violence. My testimony today, while touching upon the first issue, will deal primarily with the movement of funds. I would ask that the Committee consider this an extension of earlier testimony provided to Congress by the IPT's Executive Director, Steven Emerson.[3]

American-based operatives of terrorist groups have increasingly turned to criminal endeavors to finance their murderous actions. Whether through drug trafficking,[4] organized retail theft and black

---

[1] *Assistant Secretary for Terrorist Financing David S. Cohen, Remarks to the Washington Institute for Near East Policy,* U.S. Dep't of the Treasury (April 7, 2010) *available at* http://www.ustreas.gov/press/releases/tg632.htm.

[2] For the purposes of my testimony the term "terrorist organization" refers to those entities and individuals designated by the United States government as either a "Foreign Terrorist Organization" (FTO) or "Specially Designated Global Terrorist" (SDGT). *See Specially Designated Nationals and Blocked Persons,* United States Department of Treasury: Office of Foreign Assets Control, *available at* http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf (compilation of all U.S. designation lists) (last updated September 10, 2010).

[3] *See Money Laundering and Terror Financing Issues in the Middle East: Hearing before the S. Comm. On Banking, Housing, and Urban Affairs* (July 13, 2005) (Statement of Steven Emerson, Executive Director, The Investigative Project on Terrorism) *available at* http://www.investigativeproject.org/documents/testimony/19.pdf.

[4] *See e.g., Fact Sheet: Dawood Ibrahim,* United States Department of the Treasury, *available at* http://www.ustreas.gov/press/releases/reports/fact_sheet.pdf.

market smuggling,[5] the production and sale of counterfeit name-brand goods,[6] or car theft rings,[7] terrorists have demonstrated that they are willing and able to resort to the types of activities normally reserved for ordinary street gangs for financial support. U.S. law enforcement has and should continue to stop these activities with the same tried and true techniques that it has always relied upon to combat illicit financial activity. Those efforts, however, must be accompanied by measures aimed at preventing the actual flow of money supporting terrorism.

The United States and its international partners have effectively closed off the formal financial sector to terrorist groups. Through a combination of criminal prosecutions, regulatory enforcement, and civil litigation, traditional banking methods are no longer open to terrorist dollars. But these actions have not stopped the movement of funds by terrorist groups and their financial supporters. Instead, like water on concrete, terrorist dollars have found the cracks.

Terrorist groups have fallen back on traditional methods of financing their activities. As they did a decade ago, terrorists continue to abuse the charitable sector by raising funds under the guise of zakat (Islamic tithing) and surreptitiously funnel money to terrorist groups around the world. While this is most brazenly seen today in the form of British-based Viva Palestina's support for Hamas, we have recently seen Somalia-based al-Shabaab and Pakistan-based Lashkar-e Tayyiba do the same. Relying upon the extensive and largely unregulated hawalanetwork in the United States,[8] terrorist groups are believed to have secretly funneled hundreds of thousands of dollars over the last decade; demonstrated most recently by the September 2010 arrest of Mohammad Younis for using the technique to transfer money to Faisal Shahzad, the failed Times Square bomber.

Rather than simply rest on their laurels, terrorist groups have shown an incredible ability to adapt and apply changing technologies to their needs and stay one step ahead of our regulatory and law enforcement officers. The creation of Stored Value Cards (SVCs) and the expansion of the Internet are just two of the problems that those tasked with countering terrorist financing will face over the next decade.

I. KEEPING THE FORMAL FINANCIAL SECTOR CLOSED TO TERRORIST DOLLARS

Since 2001, the United States and its international partners have effectively closed off the formal financial sector to terrorist groups. Through a combination of criminal prosecution, regulatory enforcement, and civil litigation, traditional banking methods are no longer open to terrorist dollars.

---

[5] *See e.g., Leader of Organized Retail Theft Ring Convicted,* U.S. Dep't of Justice (April 6, 2004) *available at* http://web.archive.org/web/20051106025523/http://www.usdoj.gov/usao/txn/PressRel04/ghali_convict_pr.html.

[6] *See e.g., Id.*

[7] *See e.g., United States v. Amawi,* Superseding Indictment (Feb. 27, 2007) *available at* http://www.investigativeproject.org/case/105.

[8] *Hawala* is an underground "ancient banking system originating, and still used widely in the Middle East and Southeast Asia" *See Hawala and Underground Terrorist Financing Mechanisms: Hearing Before the S. Subcomm. On Int'l Trade and Fin,* 107th Cong. 45-49 (2001) (statement of Patrick Jost, SRA International). *See also Terrorist Financing Typologies Report,* Financial Action Task Force, at 21 (Feb. 29, 2008) *available at* http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf (explaining that terrorists exploit *hawala* and other alternative remittance systems in order to move money).

However, as I will discuss, there are still significant gaps that must be improved upon to truly make the formal financial sector off limits to terrorist organizations.

A. Regulating Formal Financial Institutions

Five years ago, Barry Sabin, then head of the Counterterrorism Section at the Department of Justice told the Senate Judiciary Committee that in order to ensure continued survival, "terrorists need to raise funds, open and use bank accounts, and transfer money."[9] Since that time, in concert with the Department of the Treasury, the Justice Department has implemented a comprehensive enforcement scheme. Although the government has not obtained a single conviction against financial institutions for terrorist financing, regulatory efforts have been both robust and effective.

At the forefront of the regulatory reforms were the amendments to the Bank Secrecy Act that accompanied the USA PATRIOT Act.[10] The updated rules and regulations have increased exponentially the breadth and depth of financial intelligence available to law enforcement officials. Today, through Currency Transaction Reports (CTRs), Cross Border Currency and Monetary Instrument Reports (CMIRs), and Suspicious Activity Reports (SARs), investigators can effectively undertake both reactive and proactive terror finance investigations.[11] Two recent examples of the applicability of these tools are the criminal prosecutions of Abdurahman Alamoudi and Pete Seda.

In 2004, Alamoudi, the former head of the American Muslim Council, pled guilty to illegal financial dealings with Libya to his involvement in a plot to assassinate then Crown Prince Abdullah of Saudi Arabia.[12] The investigation, which was triggered in part by Alamoudi's failure to file a CMIR, resulted in his receiving a 23-year prison sentence. Pleading guilty, Alamoudi admitted that he had provided hundreds of thousands of dollars to men who had been hired by the Libyan government to assassinate Crown Prince Abdullah.[13]

Earlier this month, a jury in Eugene, Oregon convicted Pete Seda, the former head of the U.S. branch of al Haramain Islamic Foundation of conspiring to move money out of the United States without declaring it, and with filing false tax returns to hide the fact that the money ever existed.[14] According to evidence presented at his trial, Seda accepted a large donation intended to support "our Muslim brothers in Chychnia," [sic] and then surreptitiously shifted the money to Saudi Arabia in the form of difficult to trace traveler's checks. Seda's co-conspirator, Soliman al-Buthe, a Specially Designated Global Terrorist, failed to file a CMIR on his way from New York to Saudi Arabia.[15]

---

[9] *A Review of the Material Support to Terrorism Prohibition: Hearing Before the S. Comm. on the Judiciary,* 109th Cong. (April 20, 2005) (statement of Barry Sabin, Chief, Counterterrorism Section of the Criminal Division, Department of Justice).

[10] United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

[11] *See generally Bank Secrecy Act Forms and Filing Requirements,* Financial Crimes Enforcement Network, *available at* http://www.fincen.gov/forms/bsa_forms/.

[12] *United States v. Alamoudi,* Plea Agreement (E.D.Va. 2004) *available at* http://www.investigativeproject.org/documents/case_docs/167.pdf.

[13] *United States v. Alamoudi,* Statement of Facts (E.D.Va 2004) *available at* http://www.investigativeproject.org/documents/case_docs/220.pdf.

[14] *Defendant Convicted of Lying About Funds Bound for Religious Extremist Militants,* Department of Justice (Sept. 10, 2010) *available at* http://portland.fbi.gov/doipressrel/pressrel10/pd091010.htm

[15] *Id.*

While the cases against Seda and Alamoudi are representative of the effectiveness of these expanded reporting and recordkeeping requirements, they are not exhaustive. Rather, they are in addition to presumably countless investigations that were triggered by the filings of CTRs and SARs.

The result of these extensive reporting requirements has been a more secure financial system. Recognizing the central role bankers play in inhibiting terrorist financing, and the difficulty associated with monitoring individual transactions to determine the final destination of otherwise innocuous funds, financial institutions have implemented these more rigid oversight systems.[16]

Despite these successes, more can and should be done to increase cooperation between law enforcement and the private sector. Although the idea has been proposed in the past, I would urge the Committee to consider working to increase information sharing with banks by granting bankers access to classified records. The inherent risks in such a proposal are obvious, but through careful monitoring I believe such a move would increase the effectiveness of terror finance investigations.

B. Holding Banks Liable for Terrorist Financing

While the Executive branch has cracked down on terror finance through increased regulatory enforcement, there have been parallel efforts undertaken in federal courts by American citizens injured in foreign terrorist attacks.[17] Relying on the Anti Terrorism Act of 1990 (ATA), these plaintiffs have looked to courts to hold accountable those individuals and entities that make acts of international terrorism possible.[18] Although these lawsuits remain in their infancy—at least in the legal sense that in most cases they have not progressed past discovery—the future effectiveness of similar suits is at risk due to judicial interpretations of statutory provisions.

The plain language of the "material support" statute proscribes the provision of "financial services" to FTOs.[19] While intuitively, this may be a clear and unambiguous term, it has been the subject of much debate at district courts litigating the ATA claims of victims of terrorism. In a string of lawsuits filed in New York and the District of Columbia, courts were tasked with interpreting the scope of "financial services" as applied to financial institutions.[20] In each case, the institutions responded to charges that they acted as bankers to terrorist groups by contending that they were simply providing "routine banking services," conduct that they argued was not covered by the

---

16. *See,* Joseph M. Myers, *The Silent Struggle Against Terrorist Financing,* 6 GEO. J. INT'L AFF. 33, 35 (2005) ("The financial services sector, which had previously opposed many of the PATRIOT Act provisions, was extraordinary cooperative and patient with the United States and other countries trying to unravel the financial trail left by the 9/11 hijackers").

17 *See e.g., In re Terrorist Attacks on September 11, 2001*, 349 F. Supp. 2d 765, 780 (S.D.N.Y. 2005); *Linde v. Arab Bank,* 384 F. Supp. 2d 571 (E.D.N.Y. 2005); and *Weiss v. National Westminster Bank PLC,* 453 F. Supp. 2d 609 (E.D.N.Y. 2006). *See also* Jennifer A. Rosenfeld, *The Antiterrorism Act of 1990: Bringing International Terrorists to Justice the American Way,* 15 Suffolk Transnational Law Journal 726 (Spring 1992) (discussing attempts by American citizens to file private lawsuits against terrorist groups, and the effect that the Anti-Terrorism Act of 1990 had on those efforts).

18 The Anti Terrorism Act of 1990, 18 U.S.C. § 2333 (2002).

19 18 U.S.C. 2339A(b)(1).

20 *See e.g., In re Terrorist Attacks*, 349 F. Supp. 2d 765; *Linde,* 384 F. Supp. 2d 571; and *Weiss,* 453 F. Supp. 2d 609.

statute.[21] And while most courts have properly rejected this argument as purely semantics, this is an area where statutory authority can be easily amended for clarity.

In bringing their claims under the ATA, victims of terrorism alleged that a number of financial institutions should be held liable for providing "financial services" to foreign terrorist organizations in violation of the material support statutes. Arguably the most insidious of the allegations involving banks were those made in *Linde v. Arab Bank,* which claimed that the financial institution had conspired to finance terrorist groups by knowingly administering what amounted to a "death insurance plan" for the families of suicide bombers in Israel.[22] On approximately October 16, 2000, the *Saudi Committee in Support of the Intifada al Quds* (Saudi Committee) was established as a private charity registered with the Kingdom of Saudi Arabia, whose purpose was to support the second Palestinian *Intifada.* According to the complaint, in furtherance of this goal, Arab Bank in consultation with the *Saudi Committee* publicly announced plans to pay out 20,000 Saudi Riyals (the equivalent of about USD $5,316) to the families of terrorists killed or captured by the Israeli Defense Forces during the *Intifada.*

The maintenance of the "death insurance plan" was relatively straightforward. Following a terrorist attack, the Arab Bank and or the *Saudi Committee* would be provided the names and personal information of the individuals who were responsible. The financial institution, in consultation with the *Saudi Committee* and local representatives of Hamas and other terrorist groups, would then compile a finalized database of persons eligible for payments. The family of the terrorist could then present the bank with a death certificate and a transfer would be made to the family's account. According to plaintiffs, the *Saudi Committee* paid death benefits to the families of at least 200 "martyrs" in the first year of its existence.

While it may be clear that running a "death insurance plan" is the type of activity that would inculpate a financial institution, what about more benign practices? In *In re Terrorist Attacks on September 11, 2001*, family members of victims of the September 11 attacks filed a class action lawsuit under the ATA claiming that over two hundred defendants directly or indirectly provided material support to Osama bin Laden and the al Qaida terrorists.[23] Among the financial institutions sued were al Rajhi Bank, Saudi American Bank, Arab Bank, and Al Baraka Investment & Development Corporation. Although each bank was alleged to have provided specific services, the general claim was that all of the banking defendants had "provided essential support to the al Qaida organization and operations."[24] The court granted the defendant banks' motions to dismiss, explaining that there is "no basis for a bank's liability for injuries funded by money passing through it on routine banking business."[25] It is simply inexcusable to allow financial institutions that solicited and transferred funds to terrorist groups to continue operating on the grounds that their support was "routine."

As the recent Supreme Court decision *Holder v. Humanitarian Law Project* concluded, the material support law was meant to cast a wide net over the types of support and services that keep terrorist organizations functioning. While it seems clear that Congress did not intend to incorporate an

---

[21] *See e.g., Weiss,* 453 F. Supp.2d at 624 (defining "routine banking services" as "opening and maintaining bank accounts, collecting funds, transmitting funds, and providing merchant account credit card services").
[22] *Linde v. Arab Bank,* 384 F. Supp. 2d 571 (E.D.N.Y. 2005).
[23] *In re Terrorist Attacks*, 349 F. Supp. 2d at 780.
[24] *Id.* at 831.
[25] *Id.* at 833.

exception for the provision of "routine" services to terrorist groups, these cases reveal a potential weakness in future enforcement of the statute. Efforts to amend the statute and explicitly reject this attempt to narrow the interpretation of "financial services," should be taken up immediately. To paraphrase one court interpreting the statute, there is nothing routine about the provision of financial services to a terrorist group.[26]

II. TRADITIONAL TERRORIST FINANCING METHODS

Despite the United States' successes at limiting the access of the formal financial sector to terrorist groups, terror financing has not completely abated. FTOs continue to utilize long-established schemes to finance their existence and operations, including abuse of the charitable sector and informal value transfer systems such as hawala.

A. Abuse of the Charitable Sector

Perhaps one of the most common methods by which terrorist groups have and continue to raise and move money is through the abuse of the charitable sector. And while the case of the *Holy Land Foundation* is certainly the most public example of a charity being hijacked to finance terrorist operations, "charities" continue to funnel money to Hamas, al-Shabaab, and others under the guise of "humanitarian assistance."

1. Hamas has and continues to raise funds under the guise of "humanitarian efforts"

By now, the illegal activities of the Holy Land Foundation for Relief and Development (HLF) have been well documented. In 2004, HLF was charged with serving as the U.S. fundraising arm for Hamas. The Richardson, Texas-based charity funneled over $12 million to Hamas under the guise of "humanitarian relief efforts." Four years later, a federal jury convicted five former officials for providing financial assistance that was used to build Hamas-run schools, to recruit suicide bombers, and to compensate the families of "martyrs."

U.S. District Judge Jorge Solis sentenced former HLF Chief Executive Officer Shukri Abu Baker and co-founder Ghassan Elashi to 65 years in prison. Longtime HLF chairman, Mohamed el-Mezain, who was convicted on one count of conspiring to provide material support to terrorists, received the maximum 15-year sentence. Explaining the sentence, Judge Solis said "the purpose of creating the Holy Land Foundation was as a fundraising arm for Hamas."

With HLF shut down and the curtain pulled back on Hamas' abuse of the charitable sector, this FTO has had to look to other "charities" to finance its vicious crackdown on the Palestinian territories. Taking the lead has been Viva Palestina (VP).

VP, a British-based "charity" with an American branch, was established in January 2009, with the expressed purpose of providing "humanitarian assistance" to the Palestinian people. But despite this laudatory mission statement, the organization has openly used its resources to prop up the terrorist organization's government in the Gaza Strip. During a March 2009 Hamas rally in Gaza City

[26] *See, Linde,* 384 F. Supp. 2d 571.

attended by leaders from Hamas and VP, George Galloway, the head of VP handed a bag full of cash to Hamas Prime Minister Ismail Haniyeh and announced:

> "We are giving you now 100 vehicles and all of the contents, and we make no apology for what I am about to say: We are giving them to the elected government of Palestine [Hamas]. Just in case the British government or the European Union want to face me in any court, let me tell them live on television: I personally am about to break the sanctions on the elected government of Palestine. Many of my friends have to give their cash to charities. By Allah, we carried a lot of cash here. You thought we were all fat. We are not fat. This is money that we have around our waists. And we have to give this... Some of my friends have to give this money to charities, and they will do this in private later this evening, because they need receipts and it's not practical to do it here."
>
> "But I, now, here, on behalf of myself, my sister Yvonne Ridley, and the two Respect councilors – Muhammad Ishtiaq and Naim Khan – are giving three cars and £25,000 in cash to Prime Minister Ismail Haniyeh. Here is the money. *This is not charity. This is politics.*"[27]

While primarily operating out of the United Kingdom, VP conducts fundraising efforts in the United States where the organization benefits from neither corporate nor charitable status. In order to ensure these funds—which will inevitably make their way into the hands of Hamas—remain tax deductible, VP has partnered with the Interreligious Foundation for Community Organizations/Pastors for Peace (IFCO), a recognized 501(c)(3) organization. Explaining this arrangement, Galloway said:

> "You can do it online, we will not be crossing into Gaza until the 13th. Any penny you can send between now and then, which incidentally is not coming to us but to the respected Christian organization, Pastors for Peace, who are our sponsors, no breaking of the law here, all US laws have been observed here, and complied with here."[28]

Over the past two years, VP has continued to flout U.S. terror-financing laws, raising over $200,000 for "humanitarian efforts" at events in Dallas, Texas;[29] Houston, Texas;[30] Orlando, Florida;[31] Brooklyn, New York;[32] Washington D.C.;[33] Boston, Massachusetts;[34] and Overland Park, Kansas;[35]

---

[27] *British MP George Galloway Defies International Sanctions Against Hamas and Compares Tony Blair to Caligula's Horse,* al-Jazeera TV (Qatar) (March 8-9, 2009) *available at* http://www.memrity.org/clip/en/2060.htm (emphasis added).

[28] *Viva Palestina: A Lifeline from the United States to Gaza,* Fundraiser at American University (Washington, D.C., June 28, 2009).

[29] *See Gaza Solidarity Day Event in Dallas, Texas,* YouTube (June 15, 2009) *available at* http://www.youtube.com/watch?v=YY3Vo7g29p4.

[30] *See George Galloway Speech in Houston,* YouTube (June 16, 2009) *available at* http://www.youtube.com/watch?v=mMILGEoVQaQ (In this video, Mahdi Bray, Executive Director of Muslim American Society-Freedom Foundation, suggests that donors route money through MAS).

[31] *See Busted: Orlando Mosque Finances Hamas Fundraiser,* YouTube (June 14, 2010) *available at* http://www.youtube.com/watch?v=f-HIQQMUrLc.

[32] *See Join George Galloway in Brooklyn in an Evening for Gaza,* Al-Awda NY ((Jan. 31, 2010) *available at* http://www.al-awdany.org/newsite/index.php?option=com_content&view=article&id=81:the-siege-continues-the-struggle-goes-on-the-honorable-george-galloway&catid=1:events&Itemid=2.

[33] *See George Galloway Champions a Free Palestine,* YouTube (June 28, 2009) *available at* http://www.youtube.com/watch?v=93DEUvpSchM.

among others. And while the American branch of VP denies that it provides financial support to Hamas, there is overwhelming evidence that the organization has donated funds raised on American soil to a non-governmental organization tied to a designated Hamas support entity.

VP-USA has said that the donations from its July 2009 convoy to Gaza were were "given to a non-governmental consortium in Gaza called Expertise in Consulting and Development (CODE), which was, in turn, responsible for distributing the aid in a manner consistent with our goals, as well as with the community's needs."[36] CODE, however, has received significant funding from the Union of Good, an organization headed by Qatar-based Muslim Brotherhood spiritual advisor, Yusuf al-Qaradawi, and designated in 2008 by the Treasury Department as an organization created by Hamas to "transfer funds to the terrorist organization." As the Treasury announcement noted:

> "in addition to providing cover for Hamas financial transfers, some of the funds transferred by the Union of Good have compensated Hamas terrorists by providing payments to the families of suicide bombers."[37]

The third "convoy" undertaken by VP arrived in Gaza in January of this year and raised funds at events in both the United States and the United Kingdom. In Britain, VP officially partnered with the Palestine Solidarity Campaign (PSC) whose stated mission includes campaigning for "the right of return of the Palestinian people," and opposing "racism, including anti-Jewish prejudice and the apartheid and Zionist nature of the Israeli state."[38] PSC has also rebutted the "myth" that "Hamas is an illegal terrorist organization bent on Israel's destruction," claiming instead that "Hamas is a nationalist, Islamist organization consisting of political party, with a military wing, which for years was largely responsible for running hospitals and schools in Gaza, in a situation of military occupation."[39]

Another major partner of VP during its third convoy was Foundation for Human Rights and Freedoms and Humanitarian Relief (IHH), the Turkish organization behind the deadly May flotilla raid in the Mediterranean Sea. While the raid remains under investigation by the United Nations, Israeli intelligence officials have confirmed that IHH planned the violent encounter with the Israeli Defense Forces prior to embarking on the flotilla, and that seven out of the nine men killed expressed their desires to die as martyrs.[40] The U.S. government has already recognized IHH's ties to Hamas, with the State Department reportedly debating designating the organization as a Specially

---

[34] *See Protesting George Galloway in Boston,* YouTube (Feb. 1, 2010) *available at* http://www.youtube.com/watch?v=FJeI_yJyRDk&feature=related.
[35] *See 103,000 pledged to Palestinian relief; largest event of its type in Kansas or Missouri,* Citizens for Justice in the Middle East (July 5, 2009) *available at* http://www.cjme.org/newsrelease-viva-palestina-benefit3.htm.
[36] *Viva Palestina Addresses Concerns,* Viva Palestina-USA (Oct. 31, 2009) *available at* http://www.investigativeproject.org/documents/misc/389.pdf.
[37] *Treasury Designates Union of Good,* United States Department of the Treasury (Nov. 12, 2008) *available at* http://treas.gov/press/releases/hp1267.htm.
[38] *PSC Aims,* Palestine Solidarity Campaign, *available at* [38] *PSC Aims,* Palestine Solidarity Campaign, *available at* http://www.palestinecampaign.org/Index5b.asp?m_id=1&l1_id=2&l2_id=10.
[39] *The Truth About Gaza,* Palestine Solidarity Campaign, *available at* [39] *The Truth About Gaza,* Palestine Solidarity Campaign, *available at* http://www.palestinecampaign.org/files/FAQ%20Gaza%20sheet%20final.pdf.
[40] *See Video Statements from Mavi Marmara Crew Members about Preparations Made by IHH Operatives for the Violent Confrontation with IDF Soldiers,"* Intelligence and Terrorism Information Center (June 9, 2010) *available at* http://www.terrorism-info.org.il/malam_multimedia/English/eng_n/html/hamas_e112.htm.

Designated Global Terrorist.[41] VP is currently en route to Gaza for its fifth land convoy, and has once again partnered with IHH.

Despite compelling evidence that VP and its American partners are raising and providing money to Hamas, a designated FTO, the organization continues to operate largely unimpeded in the United States. And while the risks posed by VP's continuing operation are grave, as recent investigations demonstrate, Hamas does not maintain a monopoly on the abuse of the charitable sector for the financing of terrorism.

2. Abuse of the charitable sector is not limited to Hamas

American authorities have uncovered an extensive support network in the United States for Somali-based al Qaida affiliate, al-Shabaab. In August of 2010, federal prosecutors released an indictment charging 14 people with providing money, services, and personnel to al-Shabaab.[42] While the case is ongoing, court records provide incredible insight into the lengths to which al-Shabaab's supporters have gone to funnel money to the terrorist group in Somalia.

Two of those indicted—Amina Farah Ali and Hawo Mohamed Hassan—of Rochester, Minnesota, stand accused of raising funds for the group while claiming it was for humanitarian purposes. According to public records, Ali and Hassan lied to both local media and law enforcement officials about the ultimate destination of the finances they were raising. In July 2009, they told FBI agents that they were only interested in providing "suffering people" in Somalia with food, clothing, and shelter.[43] Similarly, prior to her arrest, Ali told Minneapolis Public Radio that she sent money and "mails shipments of donated clothing to penniless refugees who are scrambling to escape the violence of her homeland." Declaring it was "my duty to help out the Somali poor people who left everything behind," Ali said she would never support any group that would carry out violent attacks in Somalia or the United States.

The indictment unsealed against the women paints a very different picture. It alleges that the pair raised money for al-Shabaab through door-to-door solicitation in Rochester, Minneapolis, and elsewhere in the United States and Canada. It states that on October 26, 2008, Ali hosted an al-Shabaab fundraising teleconference in which a co-conspirator "told the listeners that it was not time to help the poor and needy in Somalia; rather, the priority was to give to the mujahidin [holy warriors]."[44]

Ali was involved in collecting funds from people who pledged money in the Minneapolis-St. Paul area. In January 2009, she allegedly directed an unindicted co-conspirator to "always collect in the name of the poor" so the funds could go to the mujahidin. On other occasions, she directed colleagues to send the funds in order to conceal that the money was going to al-Shabaab.

---

[41] *Press Briefing,* United States Dep't of State (July 7, 2010) *available at* http://www.state.gov/r/pa/prs/dpb/2010/07/144116.htm.

[42] *Fourteen Charged with Providing Material Support to Somalia-based terrorist organization al-Shabaab,* U.S. Dep't of Justice (Aug. 5, 2010) *available at* http://www.investigativeproject.org/documents/case_docs/1360.pdf.

[43] *United States v. Ali,* Indictment (D. Minn. Aug. 2010) *available at* http://www.investigativeproject.org/documents/case_docs/1355.pdf.

[44] *Minneapolis Somalis Played Key Role in al-Shabaab Investigation,* IPT News (Aug. 6, 2010) *available at* http://www.investigativeproject.org/2092/minneapolis-somalis-played-key-role-in-al-shabaab.

At the Investigative Project on Terrorism, we have been carefully following al-Shabaab fundraising activities in North America for some time. From interviews with community residents in Minneapolis, our organization learned that the recent indictments only confirmed what many local Somalis had long suspected: that al-Shabaab operatives have been raising money from them under the false pretense by "playing the victim card."[45]

3. Refining efforts to protect the charitable sector

Each of these cases is demonstrative of the fact that terrorist groups continue to abuse the charitable sector by raising funds under the guise of "humanitarian efforts." Recognizing these abuses, it is important to redouble efforts to ensure the sanctity of the charitable sector. While law enforcement officials have made tremendous strides in protecting the charitable sector from abuse, more can and must be done. Existing statutory authorities must be protected from attempts to weaken their effectiveness, and officials should expand enforcement of existing laws.

Critics of American efforts at countering terrorist financing frequently argue that some terrorist groups maintain both charitable and militant wings, and that while support to the militant wing should be proscribed, it should be legal to provide "humanitarian assistance." While these critics have had limited success in convincing federal courts of these efforts, they were dealt a major blow in *Holder v. Humanitarian Law Project.* Prior to the ruling, critics of the material support law had argued that:

> "Allowing charities to provide humanitarian aid to individuals trapped in conflict zones in the Middle East and Central Asia, for example, would go a long way towards countering negative perceptions of America....Requiring a showing of specific intent to support illegal act prevents squandering limited prosecutorial resources on pro-peace charities such as the Humanitarian Law Project."[46]

This argument was roundly rejected by the majority of the Court, with Justice Antonin Scalia explaining: "The theory of the legislation is that when you aid any of their enterprises, you're aiding the organization. Hamas, for example, gained support among—among the Palestinians by activities that are perfectly lawful, perhaps running hospitals, all sorts of things."[47]

Having failed to convince the Supreme Court that the law itself was unconstitutional, challengers have promised to seek legislative amendments that would allow for humanitarian aid. Such efforts would have the effect of dramatically undermining efforts at keeping money out of the hands of terrorists, and should be rejected if and when they arise. "Humanitarian assistance," to the charitable, social service, and educational activities provided by FTOs can be just as dangerous as weapons.

---

[45] *See Id.*

[46] Sahar Aziz, *Protecting Speech, Preserving Charity: Why the High Court Should Refine "Material Support" Provision,* American Constitution Society (April 2, 2010) *available at* http://www.americanconstitutionsociety.org/node/15739.

[47] *Holder v. Humanitarian Law Project,* Oral Arguments, at 17 (U.S., Feb. 23, 2010) *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/08-1498.pdf.

In addition to rejecting efforts to water down the material support statute, steps should be taken to expand current enforcement of terror-finance laws as they apply to charitable institutions. The IRS must expand its review and verification of information provided in applications for charitable status; increase the frequency of audits of charitable filings; and impose stiffer sanctions for noncompliance. To assist in these efforts, more manpower should be allocated, with an effort made to draw upon the skills of criminal investigators.

Finally, with regards to Viva Palestina, efforts must be made to investigate the organization and its U.S. branch partners. Representative Brad Sherman (D-CA) urged the Justice Department, the IRS, and the Secretary of State to investigate whether Viva Palestina is raising money for Hamas in December, 2009. Similarly, in January of 2010, in a letter sent to the Treasury Secretary, Timothy Geithner, Representative Sue Myrick (R-NC) stated that the Treasury Department should designate VP under Executive Order 13224 for its support of Hamas. These efforts should be supported to ensure that money doesn't continue flowing to Hamas under the guise of humanitarian assistance.

B. Continuing Failure to Regulate Hawalas

Another tried and true method of moving terrorist finances has been underground banking. Since terrorist organizations can no longer safely use the international banking system, terrorist financiers have turned to these underground banking systems, specifically hawala. Although one obvious benefit of hawala for terrorist financiers is that it operates outside the bounds of the traditional financial system, there are many other reasons why hawala may be preferred to ordinary banks. They are reliable, efficient, anonymous, and available 24 hours a day, seven days a week.

The true extent of terrorist use of these systems is unknown, a result of both the criminal nature of the activity and the lack of systematic data collection and analysis.[48] Estimates regarding the annual flow of transactions through informal banking systems range from "tens of billions" to $200 billion.[49]

Groups like al Qaida have systematically used hawala because, unlike formal financial institutions, they neither were traditionally subject to potential government oversight nor did they keep detailed records.[50] Evidence shows "the hawala network has been used to funnel money to terrorist groups in the disputed Kashmir valley . . . [and] as a conduit for funding the 1998 bombings of U.S. embassies in Kenya and Tanzania."[51] Even more recently, reports have now surfaced that the failed Times Square bombing was financed, at least in part, through hawala transactions.

---

[48] *See* U.S. GEN. ACCOUNTING OFFICE, TERRORIST FINANCING: U.S. AGENCIES SHOULD SYSTEMATICALLY ASSESS TERRORIST' USE OF ALTERNATIVE FINANCING MECHANISMS, at 3 (2003) *available at* http://www.gao.gov/new.items/d04163.pdf ("[The FBI] do[es] not systematically collect and analyze data on alternative financing mechanisms.").

[49] *Id.* at 24.

[50] *See* JOHN ROTH, DOUGLAS GREENBURG & SERANA WILLE, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., MONOGRAPH ON TERRORIST FINANCING, at 25 *available at* http://www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf.

[51] Alan Lambert, *Underground Banking and Financing of Terrorism,* 15 FLA. J. INT'L L. 3, 12 (2002) (emphasis added).

Immediately following the failed bombing in Manhattan, investigators began unraveling the money trail to identify co-conspirators in the attack planned and financed by Tehrik-e-Taliban Pakistan (the Pakistani Taliban). As part of that investigation, questioning of Faisal Shahzad hinted that the plot had been funded through hawala. On September 15, prosecutors announced they had arrested and charged Mohammad Younis with helping finance the attack by serving as a hawaladar.[52] Prosecutors say Younis had engaged in unlicensed hawala transactions with Shahzad. Younis has been charged with the operation of an unlicensed money transfer business between the United States and Pakistan.

As the investigation into the failed Times Square bombing shows, the use of hawala remains a viable method for movement of terrorist finances. And while expanded application of Bank Secrecy Act reporting and recordkeeping requirements to hawala was a strong first step, the statute must be more aggressively enforced. Younis' prosecution is a reminder of the importance of financial investigations as part of a broader counterterrorism policy. Every terrorism investigation should include a concomitant terror-finance component.

III. POTENTIAL FOR ABUSE OF DEVELOPING TECHNOLOGIES

As I've explained, the United States has undertaken extensive efforts aimed at curbing the abuse of the formal and "traditional" informal financial networks. And yet, one need only open a newspaper to see that groups such as al Qaida, Hizballah, Hamas, and their ilk still retain the ability to effectively plan, finance, and carry out attacks. This is due, at least in part, to the fact that rather than simply rest on their laurels, terrorist groups have shown an incredible ability to adapt changing technologies to their needs and stay one step ahead of our regulatory and law enforcement officers. The creation of Stored Value Cards (SVCs) and the expansion of the Internet are just two of the problems that those tasked with countering terrorist financing will face over the next decade.

As a word of caution, in this area, we are largely talking about *suspected* vulnerability, rather than *demonstrated* vulnerabilities. But, as the title of today's hearing suggests, we must review the *evolving* nature of the threat.

A. Stored Value Cards

Historically, if a terrorist group wanted to move large sums of money from one location to another, they would need to rely upon the methods we have already discussed or resort to techniques like bulk cash smuggling. Increased recordkeeping and reporting requirements have made those all risky ventures. Technology, however, has now made bulk cash smuggling easier in the form of stored value cards (SVCs).

As the Treasury Department has explained, SVCs are "smart cards with electronic value....The technology eliminates coin, currency, scrip, vouchers, money orders, and other labor-intensive payment mechanisms."[53] Similar to gift cards, SVCs can be obtained in a variety of locations, often

---

[52] *Manhattan U.S. Attorney Charges Long Island Man with Engaging in Hawala Activity that Funded Attempted Times Square Bombing,* United States Attorney for the Southern District of New York (Sept. 15, 2010) *available at* http://www.investigativeproject.org/documents/case_docs/1375.pdf.

[53] *See Stored Value Cards,* United States Department of the Treasury, *available at* http://www.fms.treas.gov/storedvalue/.

without verification of identities, making them ideal as conduits for the global movement of funds. The implications of this development in terms of terror financing and our government's ability to combat it are simply daunting. This threat is exacerbated by the fact that while the Treasury Department is currently reviewing these new products, SVCs are not currently considered "monetary instruments" for reporting and recordkeeping purposes.

Under the current anti-money laundering and counter-terrorist financing regime, individuals must file Currency and Monetary Instrument Reports (CMIRs), whenever transporting, mailing, or shipping over $10,000 in "monetary instruments."[54] Covered instruments include: (i) coin or currency of the United States or of any other country, (ii) traveler's checks in any form, (iii) negotiable instruments including checks, promissory notes, and money orders) in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; (iv) incomplete instruments (including checks, promissory notes, and money orders) that are signed but on which the name of the payee has been omitted, and (v) securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery.[55]

SVCs are not covered under this regime, and as demonstrated by a recent case, that could be a glaring blind spot in preventing terrorists from moving money across international borders. In September 2010, a federal court in Eugene, Oregon found Pete Seda, the founder of al Haramain Islamic Foundation, guilty of conspiring to move money out of the United States without declaring it, and with filing false tax returns to hide the fact that the money ever existed.

According to federal officials, Seda accepted a large donation intended to support "our Muslim brothers in Chychnia," [sic] and then surreptitiously shifted the money to Saudi Arabia in the form of difficult to trace traveler's checks. Seda's co-conspirator, Soliman al-Buthe, a Specially Designated Global Terrorist, took the funds in the form of traveler's checks and traveled from JFK International Airport in New York City to Riyadh, Saudi Arabia, failing to declare the money before leaving. Because traveler's checks were covered by the statute and considered reportable "monetary instruments," al-Buthe committed a federal crime the moment he failed to report the money. Had he been traveling with $150,000 in SVCs rather than traveler's checks, he would not have been criminally liable.

The exclusion of SVCs as reportable "monetary instruments" is the result of financial instruments developing faster than financial regulations. And while to date there hasn't been a reported case of terrorist groups utilizing these instruments, the Treasury Department should act fast to plug this gap before terrorist financiers take advantage of it.

B. The Virtualization of Terrorist Financing

More worrisome than the occasional new financial instrument or method of transferring money, the Internet has the potential to revolutionize the process of terrorist financing. It has already been utilized to expand nearly every facet of FTO operations, from the spread of propaganda, to the planning and preparation of attacks; and as law enforcement continues to identify existing methods of financing, terrorist groups will likely adapt by exploiting many of the attributes for which the

---

[54] *See* FinCEN form 105, *available at* http://www.fincen.gov/forms/files/fin105_cmir.pdf.
[55] *See* FinCEN form 105, *available at* http://www.fincen.gov/forms/files/fin105_cmir.pdf.

Internet has become so popular—its ease of access, fast flow of information, anonymity of communications, and dearth of regulations.

Of particular concern, should be virtual worlds, which have the capacity to serve as the hawala of the 21st century. They provide many of the same characteristics as the existing IVTS networks: they are fast, inexpensive, reliable, convenient, and—most notably—discreet. Moreover, financiers no longer need to leave the comfort of their own homes to successfully transfer large sums of money to those looking to carry out horrific attacks. The development of virtual economies, along with the dearth of regulation, makes virtual worlds the new frontier in IVTS.

The ability to conduct real-time, in-world transactions in virtual currency that can then be exchanged for U.S. Dollars or other regional currencies has made virtual worlds widely popular. Virtual worlds allow users to transfer real funds in a variety of ways, including credit cards, traditional bank accounts, pre-paid debit cards, and PayPal accounts. Despite the obvious benefits of an expanding virtual economy, officials must acknowledge that this economy is no different than the real-world economy when it comes to financial crime. Virtual worlds are especially susceptible to manipulation by terrorist financiers because they escape regulation and observation by law enforcement.

The primary concern is paltry customer identification rules associated with virtual worlds. In traditional banking, customer identification procedures are implemented both during account origination and in subsequent transactions.[56] However, the nature of virtual worlds limits the ability to accurately identify customers at each of these stages, rendering all customers more vulnerable to financial crimes.

Virtual worlds are also limited in their ability to monitor individual financial transactions. Residents can buy, sell, and exchange currency in nearly unlimited amounts without any questions asked. Moreover, once a resident seeks to move funds from the virtual world and back into the real world, there are limits on the ability to properly identify the recipient of those funds.

Although a number of companies running virtual worlds have taken action to regulate their websites, it has largely been on an ad-hoc basis. Consequently, existing regulations must be updated to curb the future potential for abuse as new sites develop. Bringing virtual worlds under the umbrella of institutions covered by the Bank Secrecy Act would be the most effective. Consequently, I would recommend the following:

- *Declare Virtual Worlds with economies to be "money services businesses," and require registration with the Treasury Department.* The present interpretation of MSB includes "any person doing business, whether or not on a regular basis or as an organized business, which engaged in the transfer of funds."[57]
- *Implement know-your-customer procedures within virtual worlds as required of other MSBs under the*

---

[56] FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 4 (Oct. 12, 2005), *available at* http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/occ-bul_2005-35.pdf ("[C]ustomer identity verification during account origination . . . is important to reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions").
[57] 31 C.F.R. § 103.11(uu)(5) (2008) (defining "Money Transmitters").

[58] Such compliance programs are required of brick-and-mortar financial institutions and, while admittedly more complicated, expanding them to virtual worlds will reduce criminal abuse of these systems. Like their brick-and-mortar counterparts, virtual worlds must ensure that every avatar with virtual currency can be linked back to a verifiable name, address, and real-world bank account.

These customer identification and verification procedures, while potentially costly and time-consuming, are a necessary expense for virtual worlds looking to profit from the spread of their economies. Although this is a developing area of regulation, traditional banks implemented similar programs when shifting to online banking.[59] Once existing BSA regulations are expanded to cover virtual worlds, law enforcement and intelligence officials can begin cracking down on one of the last remaining methods for transferring funds without any recordkeeping or reporting requirements being triggered.

IV. CONCLUDING THOUGHTS AND RECOMMENDATIONS

We have come a long way since September 24, 2001, when President George W. Bush launched the first crackdown of terrorist finances in the form of Executive Order 13224.[60] Former President Bush laid out the mission ahead in very stark terms: "you are with us or you are with the terrorists. And if you are with the terrorists, you will face the consequences."[61] True to that mission, American efforts to disrupt terrorist financing schemes have put organizations such as *al Qaida* in dire financial straits. These successes, however, have been tempered by continuing blind-spots in the enforcement of existing regulations and an inability to update current laws at pace with technological advancements.

A review of the current and evolving threat posed by terrorist financing suggests that Congress should take the following actions:

- Increase cooperation between law enforcement and the private sector by granting bankers limited access to classified records .
- Refine the term "financial services" in 18 U.S.C. § 2339A(b)(1) to include "routine banking services," affirming that there is nothing "routine" about supporting terrorism.

---

[58] *See* U.S. DEP'T OF THE TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, MONEY SERVICES BUSINESSES REGISTRATION FACT SHEET n. 1, *available at* http://www.msb.gov/pdf/FinCENfactsheet.pdf (last visited Jan. 25, 2009).

[59] *See generally* FED. FIN. INST. EXAMINATION COUNCIL, AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT (Oct. 12, 2005), www.ffiec.gov/pdf/authentication_guidance.pdf (discussing the rise in online banking and the application of the BSA requirements to such new technology).

[60] President George W. Bush, *President Freezes Terrorists' Assets: Remarks by the President, Secretary of the Treasury O'Neill, and Secretary of State Powell on Executive Order 13224*, The Rose Garden, The White House (Sept. 24, 2001).

[61] Exec. Order No. 13,224, *Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism,* (2001). *See also* President George W. Bush, *President Announces Crackdown on Terrorist Financial Network, Remarks by the President in Announcement on Financial Aspects of Terrorism Financial Crimes Enforcement Network*, Vienna, VA (Nov. 7, 2001)

- Recognize that there is no distinction between the political and militant "wings" of terrorist group, and resist any efforts—in the form of a "humanitarian exception"—to water down the "material support" statute.
- Ensure the sanctity of the charitable sector by expanding audit proceedings to ensure that terrorist groups do not hijack charities.
- Investigate Viva Palestina and its American partners for their role in funneling money to Hamas in violation of federal law.
- Expand enforcement of 18 U.S.C. § 1960, and ensure that any and all individuals operating as hawaladars be registered.
- Insure that technology doesn't make it easier for terrorists to move money by finding Stored Value Cards (SVCs) to be "monetary instruments" subject to reporting and recordkeeping requirements.
- Stay one step ahead of terrorist financiers by declaring virtual worlds with real world economies to be "money services businesses" for purposes of Bank Secrecy Act regulations.

Many of the recommendations proposed today will be neither easy nor popular. But that doesn't mean they cannot assist in combating terror financing. Admittedly, we will never get this 100% right. Anybody that comes to this Committee and says that there is a fool-proof counter-terrorist financing program in place is simply being disingenuous. But despite the successes that have been registered in starving terrorists of money, more can and needs to be done.

Chairman Moore, Ranking Member Biggert, thank you very much for inviting me to testify before you today, and I look forward to your questions about this critical issue.

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

HEARING:

"A Review of Current and Evolving
Trends in Terrorism Financing"

TESTIMONY OF ERIC L. LEWIS, ESQ.

September 28, 2010

INTRODUCTION

I would like to thank Chairman Moore, Ranking Member Biggert, and the distinguished Members of this Subcommittee for the opportunity to testify today, and, I hope, to assist the Subcommittee in understanding the extraordinary events that have led to one of the largest abuses on record of the U.S. banking system and to share some thoughts about what went wrong and what steps can be taken to prevent or at least reduce the risk of such occurrences in the future.

In 27 years of law practice, I have been involved in the investigation of some of the largest financial frauds (and instances of money laundering) in history. I served as US legal counsel to the worldwide Liquidators of the Bank of Credit and Commerce International ("BCCI"), which collapsed catastrophically in the early 1990s. Currently, I represent the Joint Official Liquidators of Madoff Securities International Limited and have also been involved in other cases involving fraud, money laundering and terror finance in the Middle East, Europe, South America, South Asia, Central Asia, and Central Africa.

The fraud that brings me before Congress today is probably larger than these, involves one of the most high risk areas of the world, and raises more fundamental concerns about the soundness of the U.S. banking infrastructure and anti-money laundering (AML) and anti-terror finance policies upon which we all rely to ensure that the American financial system is not used to facilitate criminal or terrorist activity. The fraud and money laundering that I wish to address involves the sluicing of approximately $1 trillion since September 11. It was masterminded by a Saudi named Maan Al Sanea using "The Money Exchange," a single over-the-counter money remittance company based in Al Khobar, Saudi Arabia, and shell banks and companies in Bahrain, the Cayman Islands and elsewhere. The Money Exchange ran more than $160 billion through a single bank account in New York, without any apparent scrutiny by the bank or the government of the purpose or destination of these massive movements of money. The Money Exchange was a separately operated division of a distinguished Middle Eastern trading partnership, Ahmad Hamad Algosaibi & Brothers (AHAB). The $160 billion that went through the Money Exchange's account in New York is only one part of an even larger fraud. Mr. Al Sanea employed American and British bankers who assisted in implementing the scheme. The

fraud appears to have deprived its victims of more than $20 billion and involved funds transfers on a dizzying scale through the U.S. banking system. Yet there appear to have been no questions asked—not by banks, not by regulators, not by prosecutors—until the whole scheme collapsed. And even now, as the fraud has come to light, U.S. regulators and prosecutor appear willing to turn a blind eye to this enormous abuse of the U.S. banking system.

The vast sums involved here – approximately $1 trillion in transfers through New York in aid of a $20 billion fraud -- must raise fundamental concerns about the safeguards that have been put in place to prevent our banking institutions from becoming instrumentalities of terrorist financing or fraud or other financial crimes. Those who devote energy, as all of you do, to antiterrorism policy will recognize in these figures a very, very large haystack in which to detect the needle of terrorism finance. When one considers that the payments provided to failed Times Square bomber Faisal Shahzad were $5,000 and $7,000, and that the September 11 attacks required a few hundred thousand dollars – the dimensions of the challenge come very sharply into focus. We simply don't know where all the money went; but we do know this – if we could account for the vast majority of the funds, which we cannot, even a tiny percentage of $1 trillion could do incalculable damage to our country if it was sent into the wrong hands.

This is not to suggest that there is nothing that we can do because the system is so enormous and complex. Quite the contrary. These hearings today demonstrate that with vigorous oversight, searching inquiry, aggressive policies and strict, certain penalties to punish those who abuse the banking system or fail to follow the legal requirements, these challenges can be met. There are practical ways to target the suspicious haystacks and to better identify the needles within. There are constructive steps that can and must be taken to improve our chances of detecting fraud, money laundering, and terrorism finance activity within our banking infrastructure. But first, I would like to examine briefly the anatomy of this extraordinary fraud and how it depended upon the ability of an apparently super-rich Middle Eastern fraudster to use the inter-bank dollar clearing system in New York to effect giant dollar transfers for many years without meaningful supervision, oversight, or scrutiny—effectively at will. While this example is one of the largest, it only illustrates the scope of the problem and the need for action. The testimony of Simon Charlton, the lead forensic investigator into this fraud, which is also being submitted to the Committee today, will discuss the means and methods of the fraud as an illustration of the gaps in the system that need to be addressed.

ABUSE OF THE U.S. INTERBANK PAYMENTS SYSTEM

The overwhelming majority of the financial transactions involved in Al Sanea's scheme flowed through the United States, and in particular through the U.S. dollar clearing system in New York. Dollar transactions, U.S. correspondent bank accounts, and CHIPS were thus the indispensable instrumentality of Al Sanea's fraud. In fact, without the access to the U.S. dollar clearing system, the scheme could not have been successful. At its height, this scheme utilized at least 20 interbank accounts in Manhattan. The Money Exchange's main US dollar account was with Bank of America (BOA) in New York. The Money Exchange went to BOA and set up *its own* high-volume dollar clearing account. It told BOA up front that it expected to clear $15

billion through that account annually. BOA had full visibility into this account and direct contact with its customer, the Money Exchange.

The Money Exchange was purportedly a small walk-in money remittance business with seven branches based in the Eastern Province of Saudi Arabia. It also ran a small American Express franchise and owned a static portfolio of Saudi shares. It was not a bank; it was a basic hawala, assisting low-paid expatriate workers to transfer their modest earnings home, with a total transactional volume for its customers of perhaps $60 *million* per year in total. Nevertheless, it approached Bank of America and said it would like to open a correspondent account in order to transact $15 *billion* in payments annually. It should be noted that most remittances do not involve U.S. dollars at all, and that the sum total of *all* remittances from the entire Kingdom of Saudi Arabia amounted to about $21 billion in 2008, so it is difficult to see how this small business could legitimately generate $15 billion in transactional volume in a year.

At least four enormous red flags presented themselves on these facts: (i) a "high risk" region and country; (ii) a money remittance business that accepts money transfers for "walk-in" customers with whom it has no account relationship and no opportunity to do the due diligence necessary to understand those customers and their purposes in transmitting funds; (iii) a massive transactional volume; and (iv) a transactional volume vastly disproportionate to the customer's ostensible business.

One would expect—indeed, one would *demand*—under applicable "know your customer" and anti-money laundering and anti-terror finance rules, a very searching interrogation of this customer; a careful evaluation of its intended use of the account; of the source, destination, and business use of the funds flowing through; and, because the prospective customer is itself a financial institution serving the public, a thorough investigation of *its* anti-money laundering and know-your-customer policies.

Yet, in this case, our investigation has revealed no evidence of any significant due diligence or AML investigation by BOA of the Money Exchange in connection with the opening of the BOA account in 1998, or really at any time after the opening of the account – even after the imposition of much more strict anti-money laundering and know-your-customer requirements after the tragedy of 9/11. This is not to single out one bank, but banks are the first and most critical line of defense in the war against money laundering and terrorist finance. If I or any other small business owner walked into our neighborhood bank branch to open a business account, there would be an extensive protocol to find out what I did, what my payments in are, what my payments out are, what the pattern is and how that fits into what my business does. And if one month, I suddenly received double what I usually receive or large amounts move through my account, the bank would call me to find out what was going on. Under the US Patriot Act and post 9/11 regulations, such an inquiry would be mandatory, and critically important for an account maintained by a money service business like the Money Exchange.

BOA told AHAB's advisors last year that all of its pre-2001 records relating to the account were destroyed in the terrorist attacks on the World Trade Center and that it could not,

therefore, provide any records relating to the opening of the account, although we would be quite surprised if a major national bank would have maintained its sole copy of critical records in downtown Manhattan. The Money Exchange records reveal some later due diligence in connection with proposed *loan facilities* sought by the Money Exchange from BOA. But with regard to allowing an over-the-counter remittance company in the Eastern Province of Saudi Arabia to open an account with an expected $15 billion annual throughput, there appears to have been no due diligence to speak of. Certainly, a bank can and should make inquiries regarding a customer to whom it extends credit to make sure it can be repaid. But with a customer who processes transactions for handsome fees per transaction, it appears that there was no need to ask too many questions.

There is another troubling aspect of the documentary record. In September 2006, the Manhattan District Attorney announced a settlement with BOA relating to serious AML lapses in BOA's handling of an account for a South American money remittance business. BOA "acknowledged that some of its internal anti-money laundering controls were deficient" and, in addition to paying $7.5 million to the D.A.'s office, promised to revise its AML policies, cooperate with prosecutors, and abide by any changes recommended by regulators to its compliance programs. The District Attorney, Robert Morgenthau, stated with characteristic wisdom, that "[u]nlicensed and unregulated money services businesses, foreign and domestic, pose a threat to the integrity of our nation's financial system and to our nation's safety. The banks and other financial institutions should be our first line of defense against illegal money entering the banking system. Today's settlement reminds us all of the importance of making sure that our financial institutions know the customers with whom they do business and that they adequately assess the risks associated with those customers." BOA agreed to continue working with the DA's investigation of "offshore remittance systems" including "casas de cambio, offshore money service businesses and money remitters" and their "role in international money laundering in and through New York County." The flow of funds through the BOA account in question over four and a half years was said to be "over $3 billion."

Literally at the same time it was under investigation and was negotiating this settlement with the DA's office, BOA was in communication with the Money Exchange, which was running about a $20 billion annual volume at that time. BOA asked the company to change its name to something without the words "Money Exchange," which might be a red flag to BOA's auditors or compliance officials. BOA also asked the Money Exchange to cease engaging in walk-in money remittance business. But this aspect appears to have been perfunctory and not to have been followed up. The Money Exchange simply proffered a new name not suggestive of money remittance services—it went from "Ahmad Hamad Algosaibi Brothers Money Exchange, Commission and Investment" to "Ahmad Hamad Algosaibi Brothers Finance, Development and Investment." It went right on doing walk-in remittance business. Its enormous movement of funds through its account at Bank of America remained unchanged. The truth is that if BOA had done its due diligence, it would have been immediately obvious that the throughput in the account actually had nothing to do with any money remittance business. And even the $15 billion a year predicted transaction volume was substantially exceeded. So BOA failed to ask

why a money exchange would need to process $15 billion per year and went it started to process in excess of $20 billion or $30 billion per year, it failed to ask why there was an additional $5 or $15 billion per year in transactions. On a per transaction fee basis, this was all good, no-risk business for BOA.

The nature of the fraud required money to be cycled around, and much of the $160 billion that went through Bank of America represents debt service on and repayments of existing loans, new drawings, movements of money from the Money Exchange to other group entities also controlled by Al Sanea, and other movements, as well as some overnight placements, and most importantly the misappropriation of billions of dollars by Al Sanea. But by any measure, these are stunning dollar flows for a Middle Eastern money remittance business, even assuming it handles some transactions relating to its share portfolio or between companies within the AHAB group. The transaction volume in the BOA account is, of course, also only a fraction of the overall transaction volume relating to the fraud. We have partial sets of the correspondent account statements for other entities controlled by Al Sanea – Awal Bank and The International Banking Corporation (TIBC) – both located in Bahrain -- that suggest a combined volume of well in excess of half a trillion and probably close to one trillion U.S. dollars from mid 2003 to mid 2009 for the three entities. TIBC, for example, was the fourth largest wholesale bank in Bahrain at the time of its collapse. Yet its loan book was entirely a product of Al Sanea's fraud. Its sole purpose was to take loans from banks and then funnel the funds to Al Sanea through dummy borrowers. Awal Bank was equally a creature of Al Sanea's fraud and was, further, the bank of choice for the children of a foreign head of state who appeared to be using Awal Bank to launder funds.

As Mr. Morgenthau remarked in 2006, concerning the $19 billion in overall transaction flows revealed by his investigation of South American money service businesses that banked in New York (including one that banked at Bank of America), "[t]his enormous flow of money poses a grave risk to our security. It is also apparent that much more needs to be done, particularly by banks and other financial institutions, to know with whom they are doing business." Now the sums are much, much larger, the risks much graver, and it does not appear that more is being done. Had Bank of America taken basic steps to ascertain what the Money Exchange's business was, who its customers were, and the sources and uses of the funds, this fraud might never have happened or at least it would have been stopped much earlier. Again, I am not singling out one bank. Every bank needs to know that no matter how good the business, banks must be the gatekeeper and they must have systems and oversight that cannot be ignored. The fact that the accountholder is far away does not mean that the compliance department in the U.S. needs to do less, it probably means compliance needs to do more. Red flags must be recognized and investigated with diligence if security is to be maintained. If the region is high risk; if the financial transactions far exceed the volume that should be expected in the particular business; if the pattern of transactions is circular or otherwise suspicious; banks have to have systems in place to identify the risk factors and incentives to follow up with their customers. Anti-money laundering and anti-terror finance rules not only protect our country's security, they also protect against fraud and other criminal wrongdoing.

PROBLEMS AND SOLUTIONS

U.S. anti-money-laundering and anti-terror finance policy is a two-part defense, involving pre-event diligence by banks (backed by regulatory oversight and supervision) and post-event law enforcement where that diligence fails to detect or prevent money laundering. No system can protect itself from dirty money, fraud, or terror finance without diligent banks implementing their policies strictly and without consideration of how much profit the business generates. No system can protect itself without bank regulators that care as much about the abuse of the system as about the quality of the bank's assets. Clearly, the diligence element has failed here. If BOA could not or did not identify a problem on these facts, it is difficult to have high confidence in what Mr. Morgenthau called our "first line of defense." And if the regulators are not providing an essential check to ferret out accounts that have the red flags of money laundering, then the United States banking system will be the bloodstream that sustains global crime. It doesn't matter if the money is drug money from Latin America or terror finance from the Middle East or human trafficking profits from Southeast Asia or Southeast Europe. Dollars are the most common and important currency in the world and dollars all come through the United States. It is the responsibility of the United States banks and regulators to police the system with diligence.

I do not mean to single out BOA. Some banks do better than others, but the problem is systemic, and lies in the fact that the policeman is heavily incentivized to look the other way. I speak periodically to groups of bankers overseas about U.S. AML compliance, and we hear the same thing on both sides of the ocean: compliance officials within banks want to do their jobs but are too often regarded as the "Anti-Business Department" and marginalized from the important decision processes. Part of the goal of AML policy is to strengthen the hand of these good people in the internal debate that occurs within banks. There is also the problem of dollar accounts opened in New York for foreign clients when the New York office has no real relationship with the client and the relationship officer is based elsewhere. In this case, although bank officials in New York were designated for the account, the relationship was centered in London and the Middle East. Circumstances such as these complicate the compliance relationship between bank and customer: relationship managers based elsewhere do not have the same incentive to ensure the customer's compliance with U.S. banking regulations, and U.S. bank officials may be wary of damaging a business relationship based in an overseas office.

We have seen some movement by regulators recently to put teeth into administrative fines and thus equalize the incentive structure. But we are not yet there. Although fines involving numbers such as half a billion dollars sound impressive, they have to be evaluated by reference to the underlying business, and that business is extremely lucrative. They also have to be evaluated in terms of the rigor of the regulatory regime; the likelihood that the bank gets caught is as important as the amount of the fine. The bottom line is that fines are still viewed by banks as unlikely to occur, and if they do occur, they are a cost of doing business, and, until that changes, banks will not be good policemen. In this context, it is impossible to ignore that BOA took steps to suppress any red flags that might have been raised by the Money Exchange account

at the very time that Mr. Morgenthau's office was investigating its compliance policies. So, at the time that BOA's incentive to police its accounts was at its height, it focused its attention instead on preserving its business relationship. Asking a customer to change its name to avoid scrutiny is not a discharge of a bank's Know Your Customer obligations. It is the very opposite.

Our regulatory regime also needs to make clear that if banks agree to open dollar accounts for customers, it doesn't matter if the relationship is based elsewhere, that customer must be subject to all of the scrutiny and rigor applied to someone who walks off the street in midtown Manhattan. Indeed, when the customer is in a high-risk part of the world, the customer should be scrutinized even more closely. With correspondent banking, due diligence in respect of the customer's customers is even more important. Out of sight out of mind is a recipe for disaster in international banking.

We are not aware of any investigations ongoing by the relevant regulator here: the Office of the Comptroller of the Currency (OCC). Nor are we aware of activity at FinCen concerning these events. We have met with officials at the Department of the Treasury and offered our assistance. I hope that that offer will be taken up.

Our experience on the second line of defense, criminal investigation and prosecution, has also been illuminating—and sobering. We understand that Congressman Peter King wrote to the Department of Justice, but we have received no requests for further information since then. All the prosecutors with whom we have spoken have raised similar concerns: (i) the case is large and complicated; (ii) it will be expensive and resource-intensive to investigate and charge; (iii) witnesses and documents are in many foreign countries (though all of our client's documents are available as are many of the key individuals who have cooperated with our investigation); (iv) the scheme involved a number of other jurisdictions, including Switzerland, Saudi Arabia, Bahrain and the Cayman Islands; and (v) the victims are primarily outside the United States.

These concerns are understandable, but they do not justify or excuse inaction. The US banking system was at the heart of the fraud. The United States *alone* possesses the resources and the tools to protect the global financial system from the perils of international financial crime, money laundering and terror finance. This fraud involves more than a dozen countries around the world—the United Kingdom, Switzerland, the Cayman Islands, Saudi Arabia, Bahrain, Qatar, Kuwait, Oman, the United Arab Emirates, France, Germany, Luxembourg, and Liechtenstein. Each of them has only a piece of the fraud; each can plausibly claim it only has the ability to see and investigate a small piece of a larger global problem; each can claim that some other country has the greater responsibility. But if international fraudsters and money launderers can cross borders with the click of a mouse and the response is a collective, "it's not our responsibility," this is a recipe for disaster. If the United States does not take on this responsibility, it will both undermine its own security and fail to do its part for global security interests. We would send a message to the world that it is OK to run a Madoff-sized fraud, with our banking infrastructure as its principal instrumentality, with impunity, so long as the fraudster operates from many jurisdictions and defrauds primarily foreign parties. That may be the easy response, but it is not a response whose consequences we can accept. Saudi Arabia is an

important ally in the fight against terror finance and has its own interests in stopping money laundering. I have no doubt that if the U.S. underlined the importance of getting to the bottom of this massive abuse of the U.S. financial system that was engineered by Maan Al Sanea in Saudi Arabia, Saudi Arabia would certainly cooperate.

Legislation was introduced last year and is now pending before the Financial Services Committee that would impose severe legal disabilities on offshore banking centers for allowing their banking infrastructure to be used as an instrumentality of fraud. It seems to me that we can't have it both ways. If we expect other countries to regulate their banking systems so as to prevent or detect frauds that occur outside their borders, we must take on the same obligations. If there is a growing international norm of responsibility and reciprocal cooperation among nations to prevent money laundering, the United States must be at the forefront of that evolving ethos. And that means aggressively prosecuting people who commit fraud using our banking system.

I do not think that extensive new legislation is needed. The critical need is for strong oversight and firm priorities, together with clearly defined responsibilities and accountability. The potential for regular and aggressive criminal prosecution may also change a bank's incentives. The existing federal money laundering statute at section 1956 of the Federal Criminal Code is in fact very well tailored to this situation. It specifically provides that frauds that occur abroad trigger the statute and that money laundering is a chargeable offense in the United States if *any* part of the laundering transaction took place in the US. That occurred here, in spades: Al Sanea provided false balance sheets to banks, transacted with them using forged signatures, and drew on trade finance facilities based on wholly fictitious transactions—among other things—to the tune of tens of billions of dollars. Al Sanea set up correspondent accounts in New York and rolled hundreds of billions of dollars' worth of dirty dollar transfers through them.

Many commentators have remarked upon a pendulum-like movement in AML policy over time. If the Patriot Act marked the most recent upswing, I think it is fair to say we are on the backswing today. Indeed, in preparing for this hearing, I reviewed the excellent minority staff report prepared under the direction of Senator Levin entitled "Correspondent Banking: A Gateway of Money Laundering." It observes that "[c]orrespondent accounts in U.S. banks give the owners and clients of poorly regulated, poorly managed, sometimes corrupt, foreign banks with weak or no anti-money laundering controls direct access to the U.S. financial system and freedom to move money within the United States and around the world." It further observes that, although banks extending credit to a foreign financial services institution will normally conduct due diligence into the correspondent's "management, finances, business activities, reputation, regulatory environment, and operating procedures," such due diligence often "does not occur where there are only fee-based services, such as wire transfers or check clearing." The report concludes that poor AML compliance in correspondent banking puts or financial system and our nation at risk. These findings and conclusions, published on February 5, 2001, unfortunately are

no less true today, almost ten years later, when we have learned with great regret how prescient that report was.

One must acknowledge, in fairness, that the Treasury and Justice Departments have a lot on their plates at the moment. But we have to be able to do more than one thing at a time. Powerful tools exist to address money laundering right now. They are not being used, in my view, as vigorously and consistently as they could be. In this case, we have discovered an international fraud of perhaps unprecedented proportions, involving close to a trillion U.S. dollars transiting CHIPS in Manhattan to and from Saudi Arabia and Bahrain, as well as London, Geneva, the Cayman Islands, and a number of other ports of call. We are prepared to provide full and extensive cooperation and assistance to any and all authorities that may decide to investigate this extraordinary criminal enterprise. We hope that they will.

I hope that my testimony and submissions have been helpful to the Subcommittee. We are submitting, along with this written testimony, a small selection of documents that may assist the Subcommittee in understanding Mr. Al Sanea's underlying fraud. We stand ready to assist the Subcommittee's work in whatever manner may be helpful. Thank you.

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

HEARING:

"A Review of Current and Evolving
Trends in Terrorism Financing"

STATEMENT OF SIMON A. CHARLTON
September 28, 2010

INTRODUCTION

I would like to thank Chairman Moore, Ranking Member Biggert, and the distinguished Members of this Subcommittee for the opportunity to submit testimony today. I am an English Chartered Accountant and the Managing Director responsible for Forensic and Dispute Services for Deloitte in the Middle East. I began my career with Deloitte in London working on unraveling the frauds that brought down the Bank of Credit and Commerce International, also known as "*the Bank of Crooks and Criminals.*" The work of the United States Congress, particularly the bipartisan investigation led by Senator Kerry and then-Senator Hank Brown, coupled with the work of prosecutors like New York District Attorney Robert Morgenthau, was a driving force in the detection of the fraud and the shutdown of BCCI. BCCI was a $20 billion bank, and its collapse was then the largest fraud and the largest banking collapse in history. The fraud that I am testifying about today is larger and poses far graver risks to the financial system.

After London I moved to the Cayman Islands where I continued to do investigation work focused on offshore financial institutions and investment vehicles. I then spent three years as a partner with Deloitte Financial Advisory Services in Washington D.C., where I worked on a number of large Foreign Corrupt Practices investigations. I have investigated fraud, corruption and money laundering in most parts of the world. About eighteen months ago, I started a forensic investigations practice for Deloitte in the Middle East, based in Dubai. Within months of starting this new practice I was investigating one of the largest ever frauds, one that rocked the entire banking system of the Middle East. This fraud, which has caused widespread international consternation, was conducted through a web of entities based in the Middle East, Switzerland and the Cayman Islands as well as other offshore jurisdictions. It relied on the ability of the perpetrators to move hundreds of billions of dollars, probably as much as a trillion dollars, through the United States Dollar clearing system in New York.

This huge fraud and resulting money laundering scheme would not have been possible without access to the New York interbank clearing system. While it has rocked the Middle East, it also has frightening implications for the United States and the rest of the world. Understanding the massive fraud and how the funds were laundered is critical

to identifying the risks and preserving the integrity and accountability of the US dollar clearing system. It reveals troubling flaws in the various lines of defense in the system and the crucial importance of the requirement to "know your customers' customers." Without this, the risks to the system and to society will continue to be extreme. If two banks in Bahrain and a money remittance business in Saudi Arabia can move hundreds of billions of dollars unchecked through the system, imagine how easy it could be to move and disguise the much smaller amounts required to finance other forms of illegal activity, such as terrorism and sanctions busting.

OVERVIEW OF THE FRAUD

In the early summer of 2009, Ahmad Hamad Algosaibi & Brothers Company ("AHAB"), a company located in the Eastern Province of Saudi Arabia, discovered that it was the victim of a massive Ponzi scheme and identity theft. AHAB is a family-run trading partnership that has been one of the foundations of the economy of the Eastern Province of Saudi Arabia. AHAB has had long-standing business relationships with ARAMCO and, in more recent years, partnerships with Western multinationals such as Pepsico and Crown Cork and Seal. In addition to being the exclusive Pepsi distributor for the Eastern Province, AHAB is involved in a variety of businesses including canning and bottling, can and can end manufacture, oil industry and pipeline support, shipping, stevedoring, insulation, solar energy, hospitality, and travel.

This scheme and identity theft was orchestrated by Maan Al Sanea ("Al Sanea"). Originally a Kuwaiti national, Al Sanea married into the Algosaibi family in the early 1980s and was entrusted to operate a small financial services division of AHAB. This division, known as "the Money Exchange," was primarily focused on money remittance services, which transmitted money from expatriate workers from places like the Philippines and Pakistan back to their families in those countries. It also operated a small American Express franchise and held a portfolio of Saudi shares. In modern US terms, it was a "money service business," or a "non-bank financial institution." It is also referred to in the Middle East as a "*hawala.*" These businesses do provide essential services to poor people whom most banks are not interested in taking on as customers. But these money exchanges also pose particular risks based upon their over-the-counter nature and their ability to move money across borders un-policed.

The Money Exchange was wholly controlled by Al Sanea, who, over time, walled off its operations, prohibiting communications with the AHAB partnership, intercepting mail addressed to AHAB and its partners and executives, and installing his own hand-picked managers – often experienced bankers from the United States and Great Britain. He used this complete and autocratic control to perpetrate one of the largest financial frauds in history.

In essence, Al Sanea's Ponzi scheme consisted of two steps. First, he borrowed in excess of US $9 billion from over 100 international and Middle Eastern regional banks based upon the name and reputation of AHAB, using forged signatures of the AHAB chairman. Second, he misappropriated the proceeds through various types of transfers

out of the Money Exchange and into his own corporate group, the Saad Group. Billions of dollars were borrowed without authorisation and stolen in this manner. But theft on so vast a scale would have been impossible without Al Sanea's ability to move hundreds of billions of dollars freely through the New York - based US dollar clearing system. In addition to the Money Exchange, funds were also raised through two regulated institutions in Bahrain and parts of the Saad group, which were based in Saudi Arabia and in offshore jurisdictions. Very often these funds were then transferred into the unregulated money remittance business in Saudi Arabia through the US dollar clearing system and then stolen or used to continue to perpetrate and fund the scheme. It is clear that without access to dollar clearing, this scheme would not have been possible.

Al Sanea's forgery operation was highly sophisticated, involving high-tech equipment and expert personnel. One the world's leading forensic examiners who has reviewed signatures on many of the loan documents has so far identified nearly five hundred loan-related documents that were likely forged. In addition to these findings by Dr. Audrey Giles, head of the Giles Document Laboratory and formerly head of the Questioned Documents Section of the UK Metropolitan Police Forensic Science Laboratory, often referred to as "Scotland Yard." Similar findings have been made by a government document examiner in Bahrain and other experts. These documents represent billions of dollars in unauthorized lending. The forgery was undertaken by a sophisticated process of copying or scanning signatures from document to document, so that many documents bear signatures that are exact copies of signatures on other documents.

Once funds had been borrowed or obtained from banks - approximately $9.2 billion on the AHAB side from some 118 banks on 5 continents, in most cases with no due diligence or security to speak of - Al Sanea employed a variety of fraudulent methods to channel funds to and then misappropriate them from the Money Exchange. Some of these methods were simple: Al Sanea merely wrote cheques on the Money Exchange's accounts payable to himself or his companies or withdrew cash from the Money Exchange's remittance operations in its seven branches. For example, more than $2 billion dollars were taken from the Money Exchange in the form of cheques signed by Al Sanea personally, which were drawn on the Money Exchange operational account and made payable to Mr. Al Sanea's Saudi contracting company. These cheques were drawn practically every day, in amounts reaching $1 million per day. Others were more complex, and included phony trade finance deals involving fictitious transactions and purported deliveries of goods which never actually occurred. For example Al Sanea caused the Money Exchange to open letters of credit ("LCs") as payment for phantom goods purportedly supplied to AHAB. The proceeds of the LCs were paid initially to the purported suppliers, but then retransferred to Al Sanea or the Saad Group. The repayment liability was left with the Money Exchange, which would ultimately repay the amount outstanding - with no reimbursement from the Saad Group.

Al Sanea's scheme – like all Ponzi schemes required that he be able to borrow increasing amounts of money. Some of the borrowed money was available for him to siphon out of the Money Exchange. The rest of it was used to repay previous borrowing which was required to keep the scheme going. With much of the borrowing in US dollars, loans were advanced to accounts in the US and were repaid through accounts in the US. Much of the borrowing on the AHAB side was short term in nature, with the constant repayment and draw-down of facilities. Our investigations have shown that there were more than 10,000 draw-downs of facilities over a seven-year period. As a result of this massive cycling of money, our investigation suggests that hundreds of billions of dollars - and possibly as much as $1 trillion - went through various interbank accounts in New York.

How was Al Sanea able to move all these billions upon billions of dollars around the world? It was remarkably simple. Using international communication links common in banking, such as telexes, SWIFT and Reuters, and the basic software of PC Anywhere, he and his executives could move money between New York correspondent accounts for the entities in Bahrain, Al Khobar, Saudi Arabia, Geneva, the Cayman Islands and elsewhere.

In order to attract international lenders, Al Sanea also established two banks in Bahrain. He owned one, known as Awal Bank. The other, known as The International Banking Corporation ("TIBC"), he created and controlled in the name of the Algosaibi family, although they had nothing to do with it. Many international lenders prefer to lend, and will extend more credit, if the borrower is itself a regulated institution, *i.e.*, another bank. The combination of bank licensure and (in the case of TIBC) purported financial backing by the Algosaibi family proved extremely effective at leveraging finance. Another peculiarity about the fraud was the short-term nature of the transactions, including split value foreign exchange trades and short-term trade finance and commodity transactions which by their nature and frequency should have attracted attention. From the banks' perspectives, many of these transactions were favorable because they generated significant fees, and the capital requirements to support them were less demanding.

Although TIBC never had any real capital or customers or legitimate banking business, and the main asset on its balance sheet was a completely fictitious multi-billion dollar loan portfolio, it managed to borrow billions of dollars for the apparent purpose of lending to "borrowers" who never asked for any loans, never could have supported them, and never received them. For example, individuals who owned small kiosks in Saudi Arabia were purportedly applying for and being approved by TIBC for tens of millions of dollars of loans. The funds were then siphoned into the Saad Group by Al Sanea through the use of U.S. correspondent bank accounts and a diversion of the funds through the unregulated Money Exchange in Saudi Arabia.

Had any of the international banks lending money to TIBC or Awal performed even basic due diligence on them, they would have realised that they were largely shams

with no legitimate business. Given that the Money Exchange was a remittance company located in a high-risk region of the world, one would have expected substantial due diligence on its account and transactions. One would equally have expected that brand new banks like TIBC and Awal Bank would have been subject to substantial inquiry and investigation before the whole of the U.S. financial system was laid open for them.

Like other Ponzi schemes, Al Sanea's depended on new cash flow - borrowing - to allow him to steal funds, as well as to repay older borrowing. The Money Exchange did not have any underlying, profitable business operations that could sustain borrowing remotely on this scale. Money had to be borrowed at ever-increasing rates to fund the ever-increasing debt burden, as well as the direct theft of billions of dollars over several years from the Money Exchange by Al Sanea. In the end, approximately $9.2 billion was borrowed through the AHAB entities. Based upon our investigations to date, in excess of $5.4 billion was misappropriated to the Saad Group. The balance was apparently used to service debt and otherwise fund the fraud. Our investigations in this regard are incomplete and ongoing; in certain cases we are inhibited by the fact that some financial institutions refuse to release information to allow us to properly trace funds flows.

In addition to the borrowing through the AHAB named entities, Al Sanea also borrowed through his own Saad Group of companies. Using that borrowing, in 2007, he became the largest non-institutional shareholder of HSBC, one of the largest banks in the world. Although we do not have precise visibility into the figures on the Saad Group "side" of Al Sanea's fraud, the total borrowing appears to be at least equal to the amounts borrowed using the Algosaibi name. Most, if not all, of this borrowing appears to have been based on fraudulent representations to banks around the world. Again these fraudulent borrowings were moved around the world by access of the Saad group entities to the New York US dollar clearing system.

Al Sanea's fraudulent scheme, like other Ponzi schemes, collapsed under its own weight as the financial burden of the burgeoning debt service literally overwhelmed the capacity of the Money Exchange, TIBC, and related companies to borrow new money and as investments made by Al Sanea buckled during the global financial crisis.

Many banks had been taking advantage, charging high rates for short term funds; they must have known or suspected that a legitimate business organization wouldn't be funding its capital structure with seven-day loans of hundreds of millions of dollars at rates of 15 to 18% per annum. Much of the lending was short term in nature and constantly rolled over, thereby disguising the long term nature of the situation and generating significant transaction-based fees and presumably bonuses for willing bankers. Many banks also must have known that a legitimate commodities trader would not be simultaneously buying and selling commodities, borrowing money from the bank to buy the commodities, and then taking the money upon sale to be paid back at high rates a few months later. Proper due diligence of the AHAB businesses would have shown that AHAB was not in any event a commodities trader – rather a family run business operated largely without leverage. It appears that the lenders were willing to lend without proper

due diligence, without meeting the AHAB partners, without security on a name-only basis and based on fraudulent financial statements.

For many months prior to the collapse of the scheme in the Spring of 2009, Al Sanea's executives had warned him that the pace of borrowing and his siphoning of funds simply could not be sustained. Al Sanea was not, however, in a position to heed these warnings. Apparently he had leveraged the Saad Group with equally unsustainable borrowing and was facing the same insatiable demand for debt service within his own companies. Not surprisingly, he preferred his own companies to fulfilling his obligations to AHAB, the company he had been looting for years. The global financial crisis hastened the inevitable collapse: as financial institutions tightened credit in late 2008 and early 2009, Al Sanea simply could not borrow money fast enough to meet his own obligations and those he had fraudulently created (or purported to create) within the Algosaibi-related companies.

The fraud was discovered by the AHAB partners in approximately May 2009 when the Money Exchange could no longer service the unauthorized borrowing and defaulted on it. Al Sanea at that time walked away from the Money Exchange, leaving the partners of AHAB to receive default notices from banks they had never met and to address the claims of more than one hundred financial institutions, a number of which have since sued AHAB. As a result of these actions, a thriving business conglomerate — whose operating businesses remain healthy and viable and employ thousands of workers within Saudi Arabia — is faced with demands from lenders for moneys never utilized by AHAB and which it cannot in any event repay from its ongoing businesses. Meanwhile, banks in Saudi Arabia, the Gulf region, Europe, and elsewhere have been forced to book loss reserves totaling many billions of dollars.

In May of this year, Al Sanea's principal lieutenant and one of the major perpetrators of this fraud, Glenn Stewart, fled Bahrain, violating a travel ban imposed by the Public Prosecutor there, and has taken up residence in California. (He is a U.S. citizen.) Although Stewart is subject to arrest under an Interpol "Red Notice," there is no extradition treaty between the United States and Bahrain, and my understanding is that the United States will not arrest or extradite on the basis of an Interpol notice in the absence of a treaty or other basis for arrest. Whether law enforcement authorities in the United States will take any action against Stewart or Al Sanea remains to be seen.

From my perspective based in the Middle East, I would want to emphasize the interdependence of our systems and the indispensability of the United States financial system and dollar clearing. This staggeringly huge money laundering scheme would not have been possible without access to the New York interbank clearing system.

I know that many ask the question, why should a Middle Eastern money laundering scheme be the responsibility of the United States? Shouldn't it be the responsibility of authorities in the Middle East? If money goes from Saudi Arabia through New York and then onwards to Switzerland or Bahrain, why should the United

States care that wire transfers pulse through New York? It is an important question, but I believe the answer is quite straightforward. I believe that the financial and regulatory infrastructure in the part of the world where I work, the Middle East, has come a very long way in a short time and that everyone is doing their best. But nobody has the technological and regulatory infrastructure that the United States has. Any significant money laundering scheme involving U.S. dollars must use the U.S. dollar clearing system in New York and in the case of a dollar-based fraud like this one, the U.S. banks will see the whole cycle of the transactions. Other countries may only see the money leave, or the money arrive. If it is left to foreign regulators, the responsibility is simply too diffuse, with each country seeing its interest as insufficient or its information as incomplete. When money moves in a millisecond across borders and enforcement is divided along national lines, the money launderers and the terror financiers depend on diffusion of responsibility to allow them to exploit the system. With all the international will in the world, there is only one country that can prevent that, and that is the United States.

I am grateful to the Subcommittee for the opportunity to submit testimony concerning this important set of events. I will be happy to answer any questions that the Subcommittee may have.

○