SUSPICIOUS ACTIVITY AND CURRENCY TRANSACTION REPORTS: BALANCING LAW ENFORCEMENT UTILITY AND REGULATORY REQUIREMENTS

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 10, 2007

Printed for the use of the Committee on Financial Services

Serial No. 110–30

U.S. GOVERNMENT PRINTING OFFICE

37–207 PDF WASHINGTON : 2007

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

HOUSE COMMITTEE ON FINANCIAL SERVICES

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
JULIA CARSON, Indiana
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,
LINCOLN DAVIS, Tennessee
ALBIO SIRES, New Jersey
PAUL W. HODES, New Hampshire
KEITH ELLISON, Minnesota
RON KLEIN, Florida
TIM MAHONEY, Florida
CHARLES A. WILSON, Ohio
ED PERLMUTTER, Colorado
CHRISTOPHER S. MURPHY, Connecticut
JOE DONNELLY, Indiana
ROBERT WEXLER, Florida
JIM MARSHALL, Georgia
DAN BOREN, Oklahoma

SPENCER BACHUS, Alabama
RICHARD H. BAKER, Louisiana
DEBORAH PRYCE, Ohio
MICHAEL N. CASTLE, Delaware
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
RON PAUL, Texas
PAUL E. GILLMOR, Ohio
STEVEN C. LaTOURETTE, Ohio
DONALD A. MANZULLO, Illinois
WALTER B. JONES, Jr., North Carolina
JUDY BIGGERT, Illinois
CHRISTOPHER SHAYS, Connecticut
GARY G. MILLER, California
SHELLEY MOORE CAPITO, West Virginia
TOM FEENEY, Florida
JEB HENSARLING, Texas
SCOTT GARRETT, New Jersey
GINNY BROWN-WAITE, Florida
J. GRESHAM BARRETT, South Carolina
JIM GERLACH, Pennsylvania
STEVAN PEARCE, New Mexico
RANDY NEUGEBAUER, Texas
TOM PRICE, Georgia
GEOFF DAVIS, Kentucky
PATRICK T. McHENRY, North Carolina
JOHN CAMPBELL, California
ADAM PUTNAM, Florida
MICHELE BACHMANN, Minnesota
PETER J. ROSKAM, Illinois
KENNY MARCHANT, Texas
THADDEUS G. McCOTTER, Michigan

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

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

MELVIN L. WATT, North Carolina, *Chairman*

LUIS V. GUTIERREZ, Illinois
MAXINE WATERS, California
STEPHEN F. LYNCH, Massachusetts
NYDIA M. VELÁZQUEZ, New York
MICHAEL E. CAPUANO, Massachusetts
CAROLYN MCCARTHY, New York
RON KLEIN, Florida
TIM MAHONEY, Florida
ROBERT WEXLER, Florida

GARY G. MILLER, California
PATRICK T. MCHENRY, North Carolina
EDWARD R. ROYCE, California
RON PAUL, Texas
STEVEN C. LATOURETTE, Ohio
J. GRESHAM BARRETT, South Carolina
TOM PRICE, Georgia
MICHELE BACHMANN, Minnesota
PETER J. ROSKAM, Illinois

CONTENTS

	Page
Hearing held on:	
May 10, 2007	1
Appendix:	
May 10, 2007	37

WITNESSES

THURSDAY, MAY 10, 2007

Baity, William F., Deputy Director, Financial Crimes Enforcement Network (FinCEN)	5
Bartlett, Hon. Steve, President & CEO, The Financial Services Roundtable	22
Hernandez, Salvador, Deputy Assistant Director, Criminal Investigative Division, National Crimes Branch, Federal Bureau of Investigation, U.S. Department of Justice	6
Hodge, Megan Davis, Director, Anti-Money Laundering, RBC Centura Bank, on behalf of the American Bankers Association	23
McClain, Scott K., Deputy General Counsel, Financial Service Centers of America	26
Menzies, R. Michael Stewart, Sr., President & CEO, Easton Bank and Trust Company, on behalf of the Independent Community Bankers of America	28
Mroz, Carolyn M., President & CEO, Bay-Vanguard Federal Savings Bank, on behalf of America's Community Bankers	25

APPENDIX

Prepared statements:	
Watt, Hon. Melvin L.	38
Miller, Hon. Gary G.	40
Baity, William F.	42
Bartlett, Hon. Steve	51
Hernandez, Salvador	68
Hodge, Megan Davis	76
McClain, Scott K.	87
Menzies, R. Michael Stewart, Sr.	97
Mroz, Carolyn M.	110

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Watt, Hon. Melvin L.:	
Written responses to questions submitted to William F. Baity	121
Written responses to questions submitted to Hon. Steve Bartlett	127
Written responses to questions submitted to Salvador Hernandez	129
Written responses to questions submitted to Megan Davis Hodge	135
Statement of the California Credit Union League	140

SUSPICIOUS ACTIVITY AND CURRENCY TRANSACTION REPORTS: BALANCING LAW ENFORCEMENT UTILITY AND REGULATORY REQUIREMENTS

Thursday, May 10, 2007

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

The subcommittee met, pursuant to notice, at 9:05 a.m., in room 2128, Rayburn House Office Building, Hon. Melvin L. Watt [chairman of the subcommittee] presiding.

Present: Representatives Watt, Lynch; Miller.

Chairman WATT. Let me call the Subcommittee on Oversight and Investigations to order, and thank everybody for being here. Good morning. I understand it is a little early for us to be convening a hearing, but we got thrown a curve ball by the other committee on which I sit, the Judiciary Committee.

I am on that committee also, and we are expected to question Attorney General Gonzales today. We were originally told that hearing would start at 10:00, so we moved ours up to 9:00, thinking that there would be some overlap but not a lot, and then they moved their hearing up to 9:30.

So we may not still achieve the desired objective, but we are not going to rush through this. We want to give this the attention that it deserves. And for that purpose, my ranking member has kindly agreed to limit the opening statements to just a brief opening statement by myself, and to 5 minutes by Mr. Miller, so we will get started, and I will put myself on the clock.

We meet this morning to explore suspicious activity and currency transaction reports which are required under the Bank Secrecy Act of 1970. This is the first in what is probably going to be a series of hearings to explore suspicious activity reports and currency transaction reports, the real-life experiences of financial institutions in complying with these reporting requirements, and the utility to law enforcement that these reports have.

First, I want to welcome all of the witnesses and thank them for taking the time today to appear before this subcommittee on this very important issue. And I want to say a special thanks to Megan Hodge, who is the director of anti-money laundering for RBC Centura Bank from my home State, recognizing that all politics is local, of course.

Since 9/11, there has been increased focus on rooting out financial crimes, including terrorist financing and money laundering, and rightly so. As a result of this increased emphasis on detecting financial crimes, financial institutions have had to assume a much larger role, becoming full partners with law enforcement.

Suspicious activity reports and currency transaction reports are just two of the very important ways that the financial industry has partnered with law enforcement. Today there are millions of these reports filed annually with the Financial Crimes Enforcement Network (FinCEN). Deputy Director Baity of FinCEN is here this morning and we look forward to his testimony.

In this hearing, we hope to fully explore suspicious activity and currency transaction reporting under the Bank Secrecy Act, and figure out what works well and what doesn't, what reports are useful and which ones not so useful, if any of them are not.

We know that under the Bank Secrecy Act, financial institutions must report all transactions of $10,000 or more on a currency transaction report and report all suspicious activity on a suspicious activity report. What we do not yet fully understand is how financial institutions, including depository institutions, money services businesses, and others, actually comply with these reporting requirements, and if the guidance given to them by the regulators is appropriate and effective.

We also want to explore the practical effects of Bank Secrecy Act reporting. How do financial institutions detect suspicious activity—through the use of automated computer systems, human intelligence, or some combination? Are there increased costs to financial institutions of Bank Secrecy Act compliance, and are those costs passed on to consumers? How do financial institutions train their staff to recognize and report suspicious activity? Is better guidance needed?

We also want to explore the utility of increased suspicious activity reports and currency transaction filings to law enforcement. Is law enforcement receiving robust, useful data from FinCEN and financial institutions? Are there changes that law enforcement would like to see in the FinCEN guidance to financial institutions or in the suspicious activity report form itself?

The point of this hearing is to elicit information. Understanding the full scope of the Bank Secrecy Act reporting, particularly suspicious activity reports and currency transaction reports, is a bipartisan objective. We do not have any preconceived ideas as to the utility of these reports, or have in mind any particular legislative action. Rather, we are here to learn and benefit from the witnesses' collective knowledge and experiences with Bank Secrecy Act reporting.

We all must recognize that increased Bank Secrecy Act reporting does have some cost. Financial institutions spend millions of dollars a year in compliance, some of which undoubtedly gets passed on to consumers. Americans' privacy and civil liberties must be balanced with assisting law enforcement.

We all seek to equip law enforcement with the tools they need to keep America safe, especially after 9/11. We want the information they receive, however, to be robust and effective.

With that, I will conclude and recognize the gentleman from California for 5 minutes, Mr. Miller, my ranking member.

Mr. MILLER. Thank you, Chairman Watt.

We started talking about this probably a month ago—the issues associated with the Bank Secrecy Act and how it was applied—and my staff and I have been involved in quite a few meetings and reading information. We have met with FinCEN, the bankers, and others who are involved in check cashing, as well as the FBI.

What has come out of this is obviously there is a lack of communication that is really part of the system. I mean, nobody knows what anybody else is doing, which is probably the best way to have something like this happen when you are dealing with financial institutions that are somewhat being used to hide money or transfer money that is being used for some illegal purpose.

But you try to look and you say, are the banks being overly burdened in what they are doing? Is there a need for what they are doing? Are there rules that properly define what they are supposed to do? And I think this hearing is good for one reason. I think we are going to ferret a lot of that out and determine what is working and what is not working.

I had asked some questions on the $10,000 limit, which goes back to the 1970's, and what would happen if you changed that? And it was very interesting coming out of the conversations that for every $2,000 you increase that by, you lose a lot of information out there that otherwise is needed by law enforcement. And the numbers were rather surprising when you looked at how many cases were generated by this information that is being provided.

It is rather secretive, in a way, because it is law enforcement and they are trying to determine who is doing what in this country illegally, if terrorism is occurring, if money laundering is occurring, or other crimes are being committed through the passage of currency in the form of cash.

And yet we want to look at our financial institutions and say, are we providing too much of a burden on them? Is there such a burden on a teller that when a teller does a normal transaction that teller might consider to be a normal process of his or her job, that they are filing information just out of fear rather than basically complying with what the rules might be?

I think we are going to make a lot of information public today, and it is going to be able to maybe generate some effort on our part to put these organizations and groups together to talk and see if there is a better way the system could operate, if there are things that could be changed or modified that don't impact the result of what we are trying to accomplish here.

Having met with all the parties involved, I have come to the conclusion that there is substantial information being generated that is really benefitting the safety of this country, and in many ways stopping crime that is occurring that might not otherwise be caught in other fashions.

And yet when I have talked to the individuals who are being required to do all the correspondence and apply with the system as it is structured, they feel in many cases it is a burden being placed on them. Many of the requirements are vague and ambiguous. They are not sure what they have to do, what they don't have to

do; that many of the transactions are being dealt with out of more of a cause created by fear rather than a process that they truly understand.

On the FinCEN Web site, it states, "Working together is critical in succeeding against today's criminals. No organization, no agency, no financial institution can do it alone." I agree with that, and I am pleased that FinCEN is here today, as well as the bankers and check cashers and other groups that are here, and the FBI and other law enforcement, that everybody can talk.

We can come away, I believe, with a better understanding of what we are trying to do here, what we are doing, and the benefit of that. And yet we might look at the structure and say, there are certain things we can do to streamline it, to make it more user-friendly for the banks and other agencies that have to comply with this regulation, yet do that in a fashion that does not negatively impact the positive information we are getting from the system that our law enforcement agencies will be able to work on today.

So I commend you for holding this hearing. When you first talked to me about it, I kind of scratched my head and said, yes, I have heard a little bit about this in the past from some, and it might be interesting to get the information. The more we have researched it, and the more we have talked, I think this hearing is going to be very appropriate, and I believe we will come away, hopefully, with a resolution that makes it better.

Thank you. I yield back.

Chairman WATT. Thank you, Mr. Ranking Member. And without objection, all members' opening statements will be made a part of the record. There are other members who will be joining us in progress. We are up a little early this morning for the members, I think. But that is not an indication that they are not interested. They will be here.

We have two panels of witnesses this morning, the government witnesses and then the private sector witnesses on panel two. And with their permission, I will abbreviate their introductions and assure them that I will put their full curriculum vitae into the record, but in the interest of time, just do a very brief introduction now.

On our first panel, we have William F. Baity, Deputy Director of the Financial Crimes Enforcement Network, commonly known as FinCEN. Did I pronounce Baity right? That is the way we pronounce it in North Carolina. Got it.

We also have Salvador Hernandez, Deputy Assistant Director, Criminal Investigative Division, National Crimes Branch of the FBI.

In the interests of time, and without objection, your full written statements will be made a part of the record, and each of you will be recognized for 5 minutes for a summary of your written testimony. We won't be too vigorous with that, but try to stay as close to the 5 minutes as you can and we will tap when you are in that range and getting out of bounds too far.

Mr. Baity, if you will proceed. You are recognized for 5 minutes, or somewhere in that neighborhood.

STATEMENT OF WILLIAM F. BAITY, DEPUTY DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN)

Mr. BAITY. Thank you. Good morning, Chairman Watt, Ranking Member Miller, and distinguished members of the subcommittee. On behalf of our director and the men and women of the Financial Crimes Enforcement Network, FinCEN, we appreciate this opportunity to appear today to discuss the utility of the information provided by the financial institutions in accordance with the provisions of the Bank Secrecy Act, or BSA.

As the administrator of the BSA, FinCEN continually strives to maintain the proper balance between the requirements that are imposed upon the financial services industry and the need to insure an unimpeded flow of important information to law enforcement and other officials who need this information.

This balancing effort must be ongoing, and it must be continuously reexamined. We take this responsibility very seriously, and we look forward to working with this subcommittee in our united fight to safeguard the U.S. financial system against all types of illicit financial activities. In this regard, our director has tasked everyone in the agency to take a fresh look to help reexamine the efficiencies and the effectiveness of our regulatory regimes.

I am also honored to appear today with Mr. Salvador Hernandez, Deputy Assistant Director for the Criminal Investigative Division of the FBI. Our partnership with the FBI, as well as other law enforcement agencies, allows for a seamless flow and utilization of the BSA information in our united fight against terrorist financing and money laundering.

As I discussed in greater detail in our written testimony, FinCEN works to help safeguard the financial industry from illicit financial activity. This is achieved through a broad range of interrelated activities, including: administering the Bank Secrecy Act; supporting law enforcement, intelligence, and regulatory agencies through the sharing and analysis of the information received; and building global cooperation and technical expertise among financial intelligence units throughout the world.

All of the information received pursuant to the BSA is critical to FinCEN's ultimate goal of improving the transparency within the U.S. financial system. The BSA data received through currency transaction reports, suspicious activity reports, and other forms has proven to be highly valuable to our law enforcement customers who use this information on a daily basis as they work to investigate, uncover, and disrupt the vast networks of money launderers, terrorist financiers, and other criminals.

However, FinCEN is a user in its own right. FinCEN's analysis and liaison division, which is responsible for analyzing BSA data and other information, produces analytical products supporting domestic law enforcement, intelligence, and foreign financial intelligence units.

Our analytical products range in complexity from traditional suspect-related reports to policy-level assessments of financial criminal threats in particular areas. Last year, by way of example, FinCEN produced numerous analytical products which consist of geographical threat assessments, analysis of money laundering, illicit financing methodologies, analytical support for major law enforce-

ment investigations, specific financial transactions tutorials, and analysis of the Bank Secrecy Act compliance systems.

Specific examples included our study on mortgage loan fraud, a report on domestic shell company abuse, and domestic geographic threat assessments based on requests from the Texas Department of Public Safety and the Arizona Attorney General's Office. We believe these types of analytical products, coupled with other sources, provided added value and understanding on a broader level regarding the individual reports of information that are provided under the BSA.

Our efforts also reflect the understanding that we must address these issues from an international perspective. FinCEN, a founding member of the Egmont Group of financial intelligence units, works to strengthen the international sharing of relevant financial investigation.

We, along with our FIUs, as they are called, work in a combined operational manner to better understand international threats to our responsive financial sectors. The Egmont Group has grown in 10 years from approximately 14 jurisdictions to now over 100 countries and jurisdictions having financial intelligence units like FinCEN.

In conclusion, Mr. Chairman, we are grateful for your leadership and that of other members of the subcommittee on these issues, and we stand ready to assist you in your continuing efforts to ensure the safety and soundness of our financial system. Thank you for the opportunity again to be here today, and I look forward to discussing these very important issues with the committee this morning. Thank you.

[The prepared statement of Mr. Baity can be found on page 42 of the appendix.]

Chairman WATT. You have set a tremendous precedent, ending right on 5 minutes. That is going to be a hard act to follow, Mr. Hernandez. But you are recognized for 5 minutes, or somewhere in that neighborhood, also.

STATEMENT OF SALVADOR HERNANDEZ, DEPUTY ASSISTANT DIRECTOR, CRIMINAL INVESTIGATIVE DIVISION, NATIONAL CRIMES BRANCH, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE

Mr. HERNANDEZ. Good morning, Mr. Chairman, Ranking Member Miller, and members of the subcommittee. On behalf of the Federal Bureau of Investigation, I am honored to appear before you today to discuss how the FBI utilizes information obtained from the private financial sector.

Chief among the investigative responsibilities of the FBI is the mission to proactively neutralize threats to the economic and national security of the United States of America. Whether motivated by criminal greed or radical ideology, the activity underlying both criminal and counterterrorism investigations is best prevented by access to financial information by law enforcement and the intelligence community.

The FBI considers this information to be of great value in carrying out its mission to protect citizens of this country, and over

the past 5 years, we have made significant advances in utilizing this information to carry out that mission.

In the "criminal greed" model, the FBI utilizes a two-step approach to deprive the criminal of the proceeds of his crime. The first step involves aggressively investigating the underlying criminal activity, which establishes the specified unlawful activity requirement of the Federal money laundering statute, and the second step involves following the money to identify the financial institutions used to launder proceeds of criminal activities.

In the counterterrorism model, the keystone of the FBI's strategy against terrorism is countering the manner in which terror networks recruit, train, plan, and effect operations, each of which requires a measure of support. The FBI established the Terrorist Financing Operations Section, or TFOS, of the Counterterrorism Division on the premise that the required financial support of terrorism inherently includes the generation, movement, and expenditure of resources, which are oftentimes identifiable and traceable through records created and maintained by financial institutions.

The analysis of financial records generated by the private financial services sector provides law enforcement and the intelligence community with real opportunities to proactively identify criminal enterprises and terrorist networks and disrupt their nefarious designs.

Money laundering has a significant effect on the global economy and can contribute to political and social instability, especially in developing countries or those historically associated with the drug trade. The International Monetary Fund estimates that money laundering could account for 2 to 5 percent of the world's gross domestic product.

In some countries, people eschew formal banking systems in favor of informal banking transfer policies. Systems such as hawalas or trade-based money laundering schemes, and the Colombian black market peso exchange, which the Drug Enforcement Administration estimates is responsible for transferring $5 billion in drug proceeds per year from the United States to Colombia, are chief among them.

Hawalas are centuries-old remittance systems located primarily in ethnic communities and based on trust. In countries where modern financial services are unavailable or unreliable, hawalas fill the void for immigrants wanting to remit money home to family members, and unfortunately, for the criminal element to launder the proceeds of illegal activity.

There are several more familiarized venues that criminals use to launder the proceeds of their crimes, the most common of which is the U.S. banking system, following by cash-intensive businesses like gas stations, convenience stores, offshore banking, shell companies, bulk cash smuggling operations, and casinos.

Money services businesses such as money transmitters and issuers of money orders or stored value cards serve an important and useful role in our society, but are also particularly vulnerable to money laundering activities. A recent review of suspicious activity reports filed with the Financial Crimes Enforcement Network indicated that a number of significant money services businesses' filings involved money laundering or structuring.

The FBI's pending money laundering cases include examples of proceeds generated from criminal activities such as organized crime, drug trafficking, fraud against the government, securities fraud, health care fraud, mortgage fraud, and domestic and international terrorism.

By taking a two-step approach to these investigations, step one being the investigation of the underlying criminal activity, and step two being following the money, the FBI has made significant inroads into identifying the financial infrastructure of the domestic and international criminal or terrorist organizations. Once the underlying criminal activity is identified and the financial infrastructure has been discovered, the FBI has aggressively applied the asset forfeiture laws in order to seize and forfeit the proceeds of the illegal activity.

In terrorism investigations in particular, access to financial information significantly enhances the ability of law enforcement and members of the intelligence community to effectively counter threats. The lack of complete transparency in the financial regulatory system is a weakness on which money launderers and financiers of terrorism rely to reap the proceeds of their crimes and to finance terrorist attacks.

Limited access to financial records inhibits law enforcement's ability to identify financial networks and financial activities. Efforts to detect terrorist activity through financial analysis are further complicated by the fact that the funding of terrorism may differ from traditional money laundering because funds used to support terrorism are sometimes legitimately acquired, for example, charitable contributions and the proceeds of legitimate businesses.

Overcoming these challenges so that we can prevent acts of terror has increased the importance of cooperation with our partner law enforcement agencies, the intelligence community, and the private financial and charitable sectors.

If there is any doubt that law enforcement vigorously and proactively utilizes BSA data, and especially SARs, I would like to dispel that doubt right now. Federal law enforcement agencies review and utilize SARs in a proactive manner to identify both potential money laundering cases as well as money laundering trends.

Moreover, as indicated in the 2007 National Money Laundering Strategy report that was issued last week, law enforcement agencies do not review the SARs in isolation. The Departments of Justice, Treasury, and Homeland Security encourage the formation of interagency SAR review teams to review and discuss the SARs in a coordinated manner in order to exchange information and avoid duplication of effort.

There are 80 SAR review teams operating across the country analyzing BSA data to identify evidence of financial crimes and money laundering. In many cases, these groups include representatives from State and local law enforcement. The investigations resulting from these task forces frequently result in successful investigations of money laundering, fraud, drug trafficking, and other offenses. While we are limited in our ability to discuss such cases openly because of the confidentiality requirements surrounding SARs, we would welcome the opportunity to provide you with examples of such successful investigations.

In conclusion, BSA data is invaluable to the FBI's counterterrorism efforts as well as our more traditional criminal investigations. Our experience shows that terrorism activities are relatively inexpensive to carry out and that the utilization of data obtained pursuant to the BSA provides significant operational uplift.

The FBI is committed to collaborating with the committee and Congress to ascertain whether certain categories of the BSA can be reworked without harm to our investigative capabilities. The GAO is currently studying this issue, with a report due in early 2008, and the FBI has been an active participant in this study.

However, to alter the current BSA reporting requirements without careful study to determine the range of implications could be a significant setback to investigative and intelligence efforts relative to both the global war on terrorism and traditional criminal activities. Thank you.

[The prepared statement of Mr. Hernandez can be found on page 68 of the appendix.]

Chairman WATT. Thank you to both of the witnesses for your testimony.

The members of the subcommittee will now be recognized for 5 minutes each for questioning, and if we need to, we will go back for a second round. I will recognize myself for 5 minutes of questioning.

I have heard some pretty general testimony this morning, and I still am not sure I understand much about the underlying objectives that we are here for. First of all, I need to understand better the interface between the two agencies that you are here representing, FinCEN and the FBI, or FinCEN and other parts.

Mr. Baity, FinCEN is under which Department?

Mr. BAITY. We are a bureau of the Department of the Treasury.

Chairman WATT. And do these SARs and CTRS come to your agency, or do they go to the Department of Justice? How does that work?

Mr. BAITY. If I can, let me take you through the process. If a financial institution, which is covered pursuant to our regulatory authority, either files a currency transaction report or a suspicious activity report or another BSA report, that information is placed on forms that have been designed. Those forms are then put into a data system, which is maintained at the IRS ECC complex in Detroit on our behalf.

We then ensure that the information is made available to appropriate law enforcement, which is done in several ways. In the case of the FBI and other Federal law enforcement agencies, it is done through a bulk download, where that information is provided to them in bulk.

We also have arrangements with other agencies and State law enforcement where they have the ability to go into that data set, based on guidelines and procedures which we have established, to get information that they may be interested in that regard.

And so through a myriad of ways, we provide it to a range of law enforcement pursuant to our rules of dissemination of the information.

Chairman WATT. So FinCEN is kind of a clearing house for information. You get the suspicious activity reports and currency trans-

action reports, you put them into a database, and then you make that information available to law enforcement agencies. Do you do any law enforcement yourself?

Mr. BAITY. Well, as I stated, we do a couple of things. First of all, let me go back to your question. Yes, I think your characterization is correct. We do ensure that the information is provided to the appropriate law enforcement agencies.

But the information from FinCEN's standpoint is also valuable for our use because, as I indicated, we are looking at the information on a broader base, a macro level, to see what information we can glean. Some of our analytical products—for instance, the product that we recently gave to the Texas Department of Public Safety was a study based on all of the information as it related to movement of currency, and suspicious reporting along the Texas border, and it allowed them to basically make policy decisions about allocating resources in the right places.

We also use the information to provide actual threat assessments. We are in the process of completing one for Ohio, where they can look to see money laundering trends and patterns. And we also use the information to provide guidance back to the financial sector that are filing these reports to illustrate patterns of information and various statistics, so we use the information ourselves.

Chairman WATT. All right. Now, you had in 2006 17,600,000 SARs or CTRs go into some system. I am still trying to figure out, where is that information going? Is it coming to FinCEN and going into a database? Does FinCEN itself use any of that information for investigative or prosecutorial purposes, or is that further downstream with the people that you provide the information to? Do you do any law enforcement? Do you prosecute anybody?

Mr. BAITY. No. We are not a law enforcement agency. We are a law enforcement support agency. For instance, there are several ongoing matters with, for instance, the FBI and other law enforcement where they will come to FinCEN and our analysts will help them understand the data.

Chairman WATT. But you don't prosecute anything?

Mr. BAITY. No, sir.

Chairman WATT. Okay. And so the information that you get is gross information for your purposes, for the purposes of doing the 1,284 basic reports that you described in your testimony and the 176 complex reports that you described in your testimony. Is that information—that is gross information you are using. It is the cumulative information, the statistical information, rather than specific case information, specific SARs or CTRs. Is that right?

Mr. BAITY. That is correct for the majority, even though in some of the requests, we are actually looking at the specific SARs to give that information back to the requester.

Chairman WATT. All right. My time is expired. I will chase this on down the chain in the next round of questions, and I will now recognize the ranking member for 5 minutes for questions.

Mr. MILLER. Thank you. To follow up on this, when the forms are completed—how long does that take, to complete the forms before they are put in a databank?

Mr. BAITY. From the time that the forms are actually received, there are approximately 10 days before they are actually put into the database. That is the outside.

Mr. MILLER. You said one bank was concerned that this was not really being utilized because they had received one of the forms back 8 months after they made application that it wasn't filled out completely. And their confusion was if it was important, why would it take 8 months?

Mr. BAITY. I am not—

Mr. MILLER. Was this an unusual situation?

Mr. BAITY. I think that is unusual. It could have occurred as part of a regulatory oversight, when the examiner looked at it and asked a question. But normally, when the information comes in to FinCEN, in essence, basically it is in the database within 10 working—

Mr. MILLER. So if it is not complete, it is caught at that point and the bank is notified?

Mr. BAITY. Normally, there is a process to go back to the institution, yes.

Mr. MILLER. Now, when everything is in the databank, is there any portion of that that is automatically forwarded to any law enforcement agencies, like the FBI would immediately get it, or do they just have access to that databank?

Mr. BAITY. Well, different agencies—as I mentioned, we have different ways in which we deliver the information. But normally, when I say download, every day a different completed data set of new information is put out, and those agencies that are allowed to go in and extract it in bulk can pick it up immediately, just like FinCEN does.

Mr. MILLER. A question for Mr. Hernandez with the FBI. As you see the process that occurs and this information goes to the databank, is that the best process that you can see available as far as your availability of this information?

Mr. HERNANDEZ. We receive most of that information by bulk download, as Mr. Baity has indicated. It is electronically sent to us, forwarded to us. We immediately match it with our investigative data warehouse and our FBI database.

Mr. MILLER. Is that these 80 different partnership groups out there that are working on this?

Mr. HERNANDEZ. No. Those would actually be human beings getting together to talk about what they have in the way of SARs. But our investigative data warehouse and our other database systems are matched against the information that comes in from FinCEN on the SAR reports, CTRs, and immediately put to use. So in my view, the electronic transfer of that information is the most efficient way to do business.

Mr. MILLER. Now, you have 17,600,000 reports a year. Are these matches oftentimes done by a computer matching with a name, or do you have to try to have individuals go through this information and try to specifically review it to see if there is any applicability?

Mr. HERNANDEZ. Currently, most of those matches are made by computer, by links between what we have in our databases and what comes in. And that is an important point because not so many years ago, before our databases were as robust as they are

now, most of that matching had to be done by hand. And it was a difficult process. You can imagine the kinds of numbers that come into the typical field office. They are coming in by field office based on where the activity occurred.

Now the process is much more efficient, and much more streamlined, so we are able to make use of far greater numbers of SARs now than we were even several years ago. In fact, it is interesting that the issue continues to percolate the way it has over the years. In reality, we make much better use of the SARs in spite of the fact that there are many of them, much more of them, now than we did, as I said, just years ago because of the systems that we have in place.

Mr. MILLER. The workload for individuals actually increased dramatically because of the availability of the technology you have to focus on the compliance that you receive that are most beneficial to you as far as they are applying to case work?

Mr. HERNANDEZ. Right. We actually have done some things at the headquarters level to increase, even more than we currently have, our ability to analyze SARs through a SAR exploitation product that we are working with our directorate of intelligence on that is in the process of being sent out to the field so that roles are clearly defined, who will do what with SARs when they come in.

But again, to reiterate, the use we make of them now is far more comprehensive, far greater than it was even years ago.

Mr. MILLER. There have been some comments from individuals I talked to who suggested that perhaps a working group should be organized amongst different agencies to see if we could make this process work better. But you currently have the Bank Secrecy Act Advisory Group that is in place. How successful has that been, and could it be improved upon?

Mr. BAITY. Well, we think the Bank Secrecy Act Advisory Group has been extremely successful. It is a place where we can bring together—in fact, we will be meeting next week with that group—where we bring together all of the industries that are affected by our regulatory regime, law enforcement and the regulators, to discuss the issues that are before them.

Mr. MILLER. How often do you meet?

Mr. BAITY. We meet twice a year. And that has been in existence now since before 1995, and with membership changing. But it has been a place where we have been able to address many of the issues collectively, and I think it has been successful because it allows us to get a full understanding of the concerns of the financial sector.

Mr. MILLER. Well, I see my time has expired. I don't know when it expired. But thank you very much.

Chairman WATT. I am not being all that rigorous about it. We will keep going back and forth, so if you have a question you want to get in. Let me recognize myself for 5 more minutes, and we will keep this going as long as we think it is productive.

Mr. Hernandez, I am going to approach this from the other end of the spectrum. You are the recipient of this information in some form downstream from FinCEN. Does the FBI get 17.6 million CTRs or SARs, or do you get just the bulk information? What form does this information come to you in?

Mr. HERNANDEZ. I am not certain that we get 17 million, that we get everything that FinCEN gets, because FinCEN may be parceling that out to individual agencies. I would suspect that we get most of that since our jurisdiction is so broad.

Chairman WATT. Maybe I should ask Mr. Baity that, then. Do they get 17.6 million reports, too?

Mr. BAITY. To all of the agencies who have access, they have the same access to all of the records.

Chairman WATT. So basically FinCEN is dumping this into an FBI computer. FinCEN has a computer that has the information, and it dumps it into the FBI's computer daily?

Mr. BAITY. We post it daily, and then there is a process by which the FBI and others electronically come and pull it out into their system.

Chairman WATT. Pull it out selectively or just dump it?

Mr. BAITY. It is made available to them to pull the whole data information.

Chairman WATT. And does the FBI pull the whole data information, Mr. Hernandez, that you are aware of, or is it selective in what it pulls?

Mr. HERNANDEZ. Well, the information would be pulled based on the field office where the activity occurred. For example, if the entire bulk is sent to everyone, Cincinnati at least initially would be, if it is in Cincinnati, the only field office that would be interested in those. And so it would pull those down that are of interest to it because the incident occurred there.

Chairman WATT. But the FBI gets the whole pool in one location somewhere, or is it various offices of the FBI pulling from FinCEN's database? Do we know that?

Mr. HERNANDEZ. I don't know that.

Chairman WATT. Does anybody who is accompanying you know that?

Mr. HERNANDEZ. I am told that we get monthly downloads of everything from FinCEN. It goes right into our investigative data warehouse.

Chairman WATT. Monthly downloads? So this information might be 30 days old when you get it? Is that what you are saying?

Mr. HERNANDEZ. Yes. It could be.

Chairman WATT. Okay. Mr. Baity, State agencies that wanted access, are they pulling down the whole download? Is anybody pulling down the whole database that FinCEN has, or are they just going into it selectively?

Mr. BAITY. There are two kinds. The bulk download provides the capability to get the entire download.

Chairman WATT. We have established that once a month, the FBI gets a bulk download. Is there anybody else who is getting a bulk download?

Mr. BAITY. There are other agreements with other law enforcement.

Chairman WATT. Who?

Mr. BAITY. Well, we have an agreement with DEA. We have an agreement with the Secret Service. The IRS has the ability because the data is at—

Chairman WATT. I want to know whether they are getting it—

Mr. BAITY. Yes, sir. They are getting it.

Chairman WATT.—not whether they have the ability because it sounds to me like we have duplicate technology systems out here that end up getting exactly the same information. The whole bulk information DEA gets, the FBI gets once a month. You have it in your computer. Every time we build a computer system that can take 17 million pieces of information into it, it costs the taxpayer some money, and I am just trying to find out what is being done with this stuff.

Mr. BAITY. Well, if I can, let me—in terms of the bulk download, that information is made available to the Federal law enforcement agencies so that they can directly pull it down. The reason why it is available in that regard is because they have different uses of it because of their investigatory authorities. We do not determine that, so we make that available.

The other thing we do, though, is that we make it available—you asked the question—

Chairman WATT. But might it be more efficient, if they were getting the information directly as opposed to your—

Mr. BAITY. Well, they are getting it directly. They are getting it as FinCEN's data, and they are getting it directly by us putting it out. Because they have different systems in how they bridge the information, we have built a system so they can interface to get the data.

Chairman WATT. Mr. Hernandez, are there situations where this 30-day delay in getting a bulk download has any law enforcement implications?

Mr. HERNANDEZ. That point has actually been clarified for me. We have access to the information posted by FinCEN as it is entered. So we can go in and look essentially on a daily basis for information. We get a biweekly or monthly download, a dump, essentially, of all of the information. So depending on what it is we are doing, if we are looking for something in particular, we can look for it on the same day it is entered.

And Mr. Chairman, I understand from your questions and from some of the statements early on, that some of the concern has to do with what is happening with 17 million records.

Chairman WATT. That is where I am going to get to next. That is the third round of questions. But my 5 minutes has run out again, so I will go to Mr. Miller for 5 additional minutes.

Mr. MILLER. Thank you. Taking up where we left off, you said this bank advisory group meets about twice a year. And based on meetings I had with the Financial Services Roundtable, the American Bankers Association, the American Community Bankers Association, the Financial Services Centers of America, and the Independent Community Bankers Association, there is a lot of confusion amongst the groups who have to comply with the regulations.

And there are some who think that some examiners basically have told them that they have to file a certain amount or number of CTRs or SARs, or else they will be written up for lack of compliance. I guess it might be like that every community has their own local police officer who writes more tickets than everybody else, and everybody knows that one person by name.

I don't know if that is happening out there. But is there some way that you can see we can improve upon this process, maybe meeting more than twice a year or outreach or something to more involve the groups that have to comply with the regulations?

Mr. BAITY. Let me, if I can, try to answer the specific example you raised first.

The steps we have taken in conjunction with the other bank regulators is to come together and basically put together uniform guidelines on examinations to basically help alleviate the issue raised that one examiner is far out front or different than the normal. So we put that together as a manual which is being taught to all examiners to try to bring consistency to the examination process.

We think that right now, even though we are looking at everything anew, that the current frequency of the meetings makes sense. And one of the advantages, as we rotate new industries under our regulatory authority, they are brought into the Bank Secrecy Act advisory group for discussions as we go forward.

Mr. MILLER. One repeated statement from all of the organizations was that the guidelines are vague and ambiguous to such a degree that a teller is put in a position where they are almost afraid not to file a certain type of forms even though they might not necessarily be applicable because they are afraid that it can come back on them if they don't.

Is there something we can do to clarify some of this?

Mr. BAITY. Well, again, what FinCEN has done is to try to participate in the examination training to make sure that they understand, from an examiner's point, what is expected under the regulation. We meet with them regularly. We have put out guidance on that regard. So we not only meet with the regulators, but are trying to increase the guidance that we are putting out to the financial sector as well as to what are the expectations so that everyone is at least hearing the same message in terms of what we are trying to provide.

Mr. MILLER. Mr. Hernandez, is there any alternative to the current system of CTRs and SARs that you see out there that would be as beneficial as the current system we have?

Mr. HERNANDEZ. For the purposes of law enforcement and the FBI especially, 30-plus years of the Bank Secrecy Act CTR/SAR requirement has yielded tremendous results in terms of the initiation of investigations, enhancing of investigations.

I don't see an alternative system. The FBI has always been willing to discuss, and I think has, in individual contexts with banking institutions and certainly as members of groups of this sort, ways that we might streamline the process or ways we might identify things that aren't particularly helpful to law enforcement.

But I don't see an alternative. The value coming from CTRs and from SARs is simply too great. We understand that not every single CTR and every single SAR is going to yield an investigation and a conviction. But that is not different than anything else we do. We don't not look at what may not be a smoking gun lead on a terrorism case because we think it is not going to lead us to something important. We look at those things.

And so we look at everything that comes in. We make connections where we can. And time has proved that we do make connections through joining SARs from different places, from different subjects, to make better cases, more significant white collar crime cases, that yield us to results of terrorism investigations. There simply isn't any substitute for what we get in the way SAR and CTR data that I see.

Mr. MILLER. There has been a suggestion that $10,000 today is not what $10,000 used to be in the 1970's, and perhaps that number needs to be moved up. But I understand technology is different than it used to be that benefits you.

How do you think that would impact you positively or negatively if it was raised?

Mr. HERNANDEZ. Well, I would submit that $10,000 in cash or above is perhaps even more significant now than it was 10 years ago. In a largely credit and debit-based society, the fact that individuals show up at institutions with $10,000 or $12,000 or $14,000 in cash is, I think, suspicious.

Mr. MILLER. More so than it was in the 1970's?

Mr. HERNANDEZ. Possibly so, depending on who it is that shows up and where it came from, what the business is that is involved. An argument could be made, I think, if we were to look at this closely that in certain instances, the threshold could be lowered to get at what we are really interested in, and in certain instances, perhaps raised depending on what we are interested in. But I don't think it is prudent to talk about raising the threshold simply because we are 30 years down the road.

Mr. MILLER. I guess I will follow up on my next round. My time is up.

Chairman WATT. Mr. Hernandez, you talk about over 30 years of experience. Currency transaction reports have been in existence since 1970. Right? How long have suspicious activity reports been required?

Mr. BAITY. If I can answer that, the first reporting requirements were in 1996 for depository institutions. Subsequently, other industries have been brought on. So the first suspicious reporting program was started in 1996.

Chairman WATT. And that was pursuant to the statute that was passed in 1996?

Mr. BAITY. In 1994, the Money Laundering Suppression Act basically authorized it, over the next 2 years, we developed the program, and reporting actually started in 1996.

Chairman WATT. Mr. Hernandez, you were about to tell me what happens with an individual. We have been approaching this from the 17 million pieces of paper. What happens from the individual piece of paper?

Mr. HERNANDEZ. A number of things can happen. The individual piece of paper is brought into our IDW. A connection may be made there. It may be reviewed by an individual. It may be joined with some pending investigation in that field office; it may be joined with a pending investigation in another field office.

Chairman WATT. So the FBI would have some suspicion that somebody is doing something illegal, and then they would use that

person's name to go and access a CTR or SAR report on that person?

Mr. HERNANDEZ. We might look for it by name, if we have an ongoing investigation or a subject investigation. Often, though, those CTRs, those SARs, cause us to initiate an investigation. They are, after all, suspicious activity reports. That is a clue to us that there might be something we want to look at.

So many of those CTRs or SARs start an investigation. And I understand that for the financial services industry, it is difficult sometimes to understand how one individual report might lead us to an investigation, especially if it is a smaller dollar amount. The fact is that many of those—

Chairman WATT. Essentially if there are 17 million of them, I think, is the concern that people have. Is there somebody looking at each one of these 17 million CTRs and SARs?

Mr. HERNANDEZ. I am not going to tell you, Mr. Chairman, that an individual is looking at 17 million, but 17 million are being hit against business of the current system we have, our databases, to see whether there are connections.

Chairman WATT. All right. Let me just submit for the record, just so you will have it, the examination manual, the Bank Secrecy Act Anti-Money Laundering Examination Manual. This manual contains the instructions that you all have put out to the banks or financial institutions that provide the information to go into these reports?

Mr. BAITY. If I understand what you read, I believe it is the instruction manual that is put out to the regulators in terms of their procedures for examination financial institutions for compliance with the statute.

Chairman WATT. So you give these to the regulators, and then regulators take this set of directions and issue instructions to financial institutions?

Mr. BAITY. They use that to examine if the institutions are complying with the BSA requirements. When they go in and do an examination of the institutions for their purposes, which include safety and soundness, they also review them to look for compliance with the Bank Secrecy Act. That manual is a product of our joint efforts with the regulators to bring consistency as much as we can to that process.

Chairman WATT. This part of the examination process, how does an individual bank get communicated to about what they are expected to do to prepare for the examination?

Mr. BAITY. Just about every institution has what they call a compliance officer, who is responsible for understanding the Bank Secrecy Act regulations and rules. The regulators, when they do their examination, in conjunction with those compliance officers they provide the information and expectations of them to the bank itself. So every bank has in it a process for complying or persons who are dedicated to complying with the Bank Secrecy Act requirements, if that answers your question.

Chairman WATT. It does. What has happened since 1996? I mean, it seems to me that currency transaction reports can be generated electronically. Computers can do that without substantial human involvement. What has transpired since 1996? How are

banks complying, how are financial institutions, with the non-mechanical function?

CTR is a mechanical reporting function that a computer can go in and pick out. It is a cash transaction of $10,000. The computer just spits it out. The information goes. Tell me what you understand is happening in financial institutions just after 1996 aside from CTRs?

Mr. BAITY. Well, since 1996 and specifically since 9/11, what we have tried to do is enhance the electronic filing of the information from all of the institutions that are covered so that the institution is filing not in a paper format but in electronic because it makes the data—

Chairman WATT. The CTRs, though, how do you electronically file what is a personal observation?

Mr. BAITY. Well, the suspicious activity reporting, which allows for the institution to basically examine the transaction and make a judgment whether, based on their understanding of their customer, whether that transaction is suspicious. They can fill out—

Chairman WATT. So you are saying once it has been determined by a bank employee that there is a suspicious activity, you streamline the system for reporting that. I think the question I am asking is: What do you understand to be the process before that determination is made? What are the—

Mr. BAITY. The process before, which is laid out in a regulation, is that the institution basically undertakes to review this—not just a teller making a decision, but I am talking in terms of suspicious activity reporting.

Chairman WATT. Right.

Mr. BAITY. That there is an examination within the institution, and in fact, it requires notification to senior management in the institution of the intent to file a SAR. So we ask the institution to actually make a value judgment and a review before they file the report with us.

Chairman WATT. I ask unanimous consent to submit the 2006 BSA/AMC Examination Manual for the record. Without objection, it will be submitted.

[The above-referenced document is available at the following site: www.ffiec.gov/bsa—aml—infobase/default.htm]

Chairman WATT. Is there a companion set of instructions that don't go to the examiners, but go to the financial institutions themselves, or do we need to talk to the examiners about what the content of that is?

Mr. BAITY. There are—I wouldn't say a companion manual, but there are guidelines that have been provided to the industry on various questions about the compliance. And we provide that guidance as part of what we do on our Web site that is publicly available to the financial institutions because that depends on sometimes the question that comes to FinCEN when the bank asks, what do we do in this particular case?

If it looks like a question has broad application, we issue a guidance document to all of the financial institutions that this is our perspective to answer that question.

Chairman WATT. What about institutions that are not regulated? They have examiners. Do you have examiners for institutions that are not regulated under the Federal system?

Mr. BAITY. Well, no, because first of all—let me take a step back. We are only talking about those financial industries or sectors that come under our regulatory authority. If you come under our regulatory authority, if you are, for instance, a depository institution, that is done by the Federal banking regulators—the OCC, the Federal Reserve Board, etc.

But there are a range of financial institutions that we regulate, and we look to others, particularly the Internal Revenue Service, to help us with the compliance. So for instance, in the case of casinos that are under our regulatory authority, the Internal Revenue Service has a sector that actually goes out and reviews that industry for compliance.

Again, that is done in conjunction with consultation with FinCEN as to what our expectations are. We do spend a lot of time training those industries on what we expect them to do.

Chairman WATT. All right. I am going to recognize Mr. Miller for 5 minutes, not to ask additional questions, but to seek unanimous consent to submit written questions for the record so that we can get further into this, because we could be here a long time, I think, trying to understand it. We will try to be more systematic in our approach, and maybe submit written questions to these witnesses.

Mr. Miller? Five minutes.

Mr. MILLER. Thank you.

Mr. Hernandez, you suggested that in some cases, the amount could even be lower than $10,000 that would be beneficial. Could you explain that a little further?

Mr. HERNANDEZ. I can't conceive of what that would be right now. I just believe that as we have established a $10,000 threshold, it was based on something. It may be too general, in a sense. It may be too low, given certain kinds of activities, and it may be too high, given changes that have occurred over the past 6 years, certain kinds of activities.

We have strong suspicion that on the terrorism side in particular, smaller dollar amounts are probably important and a good indicator, potentially. I think in the end that $10,000 is a good balance, given where we are. I will say this, it is my firm belief that if that were raised, and frankly, if the seasoned customer proposals that are moving forward are in fact enacted, we will get less information. That is a positive thing potentially for the financial sector because they will have to report less to us. We will have less to work with. We will have less in the way of information intelligence to put together into our investigations.

I think there is a natural tradeoff, and the decision that is left with this subcommittee and, I suppose, Congress is: Where is that tradeoff? What as a society are we willing to trade for reduced numbers of submissions by the financial sector? I think it is all valuable. I don't think anybody here is proposing that it be increased. But I think it needs to be said that there is value here, and there will be something lost by changing the rules if the rules are changed, clearly.

Mr. MILLER. There are a lot of people in this country who don't like government in their life. And I know one of the questions that was asked of me, or a comment that was made to me, by a banker was the small-town farmer who went out to the auction, sold an old tractor and a pickup truck and it exceeded the $10,000 or $11,000. He went to deposit it in his account, later to find out that that had to be filed with a CTR to the government, and he just went ballistic because he was a private person.

And that really struck home. I think back to a few years ago when I went back to bury my dad in Arkansas, a little town called Japton, Arkansas. And Japton, Arkansas, has a little store with one gas pump. My brother and I walked into it, and there was a lady in the corner with a rifle leaning up against the wall with the cash register, and three elderly gentlemen sitting in these chairs rocking, staring at us as we walked in the door.

We were going to pay, and they were staring at us. And they said, well, what are you doing here? And until I told them we came to bury my dad, and they asked who he was, then we were accepted once they found out we weren't outsiders. But there are some people in this country who just do not like the government in their life. They are honest people, just trying to live their lives and they are bothered by something like this.

How does a bank deal with these type of situations?

Mr. HERNANDEZ. Well, basically I think we are dealing with a very basic problem in setting thresholds of any kind. How specific can you ultimately make a threshold? Can we account for $10,000-plus deposits with the exception of a farmer who brings in $10,000 from the sale of a tractor? There are any number of possibilities.

Mr. MILLER. But the exemption that they are required to file, they say, by and large are so time-consuming they are unusable, that it is hard for them to justify doing it in this case. And I am not arguing this. I am just saying that this is a genuine question posed by a genuine individual who has a major concern.

Mr. HERNANDEZ. Right.

Mr. MILLER. That is what some of these banks are facing out there. And some people in this country just like their privacy.

Mr. HERNANDEZ. Sure. That is a very natural tension. We understand that. We accept that. And again, it gets back to where are we as a society going to draw that line? Do we think it is important enough to be able to capture the $10,000-plus currency transactions in the general sense across the board because we think that is indicative of criminal or terrorist behavior, and in the process, draw into that some folks who clearly aren't involved in anything of the sort? It may look suspicious at the outset, but it ends up not being suspicious. Nothing happens with that information. No investigation will follow that information.

Mr. MILLER. But, see, the guy who likes his privacy doesn't understand that argument.

Mr. HERNANDEZ. That is exactly right. We understand the concern. And it is something that obviously in the FBI we deal with all the time.

Mr. MILLER. Is there any way of making the form, Mr. Baity, more user-friendly, let's say, for banks to be able to file an exemption rather than the exemption taking 15 minutes? Isn't it easier

just to hit the buttons and file it rather than having to go the exemption process that some people would prefer to use, but it is too complicated and time-consuming?

Mr. BAITY. The short answer is, we are looking anew at everything, including the forms themselves. But if I could just take a minute to go back to your original question on exemption. As you know, there are exemptions in place that have not, from our perspective, been utilized fully by the banking sector and the other reporting entities that could reduce the number of CTRs, particularly.

What we are doing is we are re-looking at those exemptions that have been in place for a while to try to get a clear understanding to see if there is something we can do to make them more usable by the financial sector as we go forward. So the short answer is we are looking at that, including such things as the forms themselves, because they have proliferated over several years.

And if I could, Mr. Chairman, just to go back to your question, institutions do have access to the examination manual.

Mr. MILLER. I would encourage you to do that if you are looking at those because that was a repeated concern, and I think that is a good direction to go. Thank you.

Chairman WATT. Let me thank the two witnesses for being here. I ask unanimous consent to allow all members of the subcommittee an appropriate amount of time, whatever that is, to submit additional written questions to the witnesses.

And we will try to do that expeditiously and do it within the parameters of our general committee rules, not outside that timeframe. Since I am a new chairman, I don't know what that timeframe is. Thirty days? Okay, within 30 days. Without objection, so ordered.

All right. We thank these gentlemen, and we will call up our second panel of witnesses. You all are going to make me miss Attorney General Gonzales, I can see that already.

Without objection, we will submit for the record the California Credit Union League statement. They are not part of this second panel, but we will put their statement in the record.

Let me thank the second panel of witnesses for being here, and with their permission, do the same as I did with the first panel, and abbreviate their introductions. We will put your full bios into the record, but we will abbreviate in the interests of time.

Our first witness is the Honorable Steve Bartlett, who is well known to all of us on the Financial Services Committee. He has testified many times. He is the president and CEO of the Financial Services Roundtable.

The rest of the second panel consists of: Ms. Megan Davis Hodge, director, anti-money laundering, at the RBC Centura Bank, on behalf of the American Bankers Association; Ms. Carolyn Mroz, president and CEO, Bay-Vanguard Savings Bank, on behalf of America's Community Bankers; Mr. Scott K. McClain, Deputy General Counsel, Financial Service Centers of America, on behalf of the Financial Service Centers of America; and Mr. R. Michael Stewart Menzies, Sr., president and CEO, Easton Bank and Trust Company, on behalf of the Independent Community Bankers of America.

We welcome each and every one of you. And as I said, your full curriculum vitae will be put in the record, and we will recognize each one of you for 5 minutes. I may be a little more aggressive than I was with the first panel, but I will try not to be unreasonable.

Mr. Bartlett, 5 minutes, please.

STATEMENT OF THE HONORABLE STEVE BARTLETT, PRESIDENT AND CEO, THE FINANCIAL SERVICES ROUNDTABLE

Mr. BARTLETT. Thank you, Mr. Chairman. Mr. Chairman and Ranking Member Miller, we very much appreciate your leadership on this, and the leadership of this subcommittee in examining this difficult but solvable problem, a problem that has been with us for some time.

Mr. Chairman, I would ask to submit for the record the annual report for M&T Bank, which is one of our companies, and has some comments in their annual report. I referred to it in my testimony.

Chairman WATT. Without objection, so ordered.

[The above-referenced document is available at the following site: http:/ir.mandtbank.com/fundamentals.cfm]

Mr. BARTLETT. Mr. Chairman, I will summarize my testimony. It is the goal of the Financial Services Roundtable and our member companies to assist law enforcement in identifying suspicious activities and making that identification usable to law enforcement.

We believe that can be done much better than is being done now. We think it can be done with a lot less disruption. But more importantly, we think that better focus and better targeting of suspicious activities in the identification and the reporting will assist law enforcement in a much greater way than they are assisted now.

Mr. Chairman, we have been calling this problem to the attention of Congress for about 4 years. We have seen no progress at all. The system continues to get worse. It is more expensive, more clogged-up, and much more inconvenient and difficult for our customers, the customers of financial institutions, to use than it was just 4 years ago when we began calling it to the Congress's attention.

Mr. Chairman, we see three basic problems. One is the very large and increasing filing of defensive SARs. That has been well-documented. The recent SAR activity report number is 62,000 suspicious activity reports filed in 1996, and almost a million filed in 2005.

We don't think the number of suspicious activities have increased by that amount since 1996, but we think those additional filings of defensive filings has increased in response to the current procedure. And that is why we think the current procedure could be improved.

Second, and this is really in the last 18 months to 2 years, we are now beginning to see an additional problem of what we call ad hoc enforcement. In response to the manual, the guidance manual that you cited, Mr. Chairman, we are now finding on a regular basis examiners who in the examination process, they begin designing with our financial institutions under the threat of—implied threat, in any event—of a potential criminal indictment, which means we listen to them very carefully.

The examiners begin to create new and customized procedures for filing and identification of SARs that do not exist anywhere in the manual, do not exist in the regulations. Indeed, there are no regulations. These are guidance and not regulations.

And so in the absence of a rule of law, in many of our companies—not all, but many of our companies—tell us that now, during the examination process every year, they just simply make up a new process for going forward, and then presumably they think that they will end up making up a new process the following year, depending on who the examiner is, which demonstrates the lack of clarity and the lack of rules in place to follow.

And third, Mr. Chairman—this is the one that is the most difficult for us—the filing of suspicious activity reports, one of the results of this is that our companies are often told that a particular account or implied that a particular account is suspicious in some way. And oftentimes, we know that it is not suspicious. Oftentimes, it is a seasoned customer, a customer we have been doing business with for a long time. But the outcome is we close the account.

And the outcome of that is you take large numbers of legitimate customers out of the banking system, which doesn't help law enforcement, but does inconvenience those customers, some consumers, some small businesses, and also is harmful to the economy because you drive more people into the unbanked system of the cash economy.

Mr. Chairman, we think that the system can be improved. I have met with most of the succession of directors of FinCEN, and they all have good intentions. I have also met with several Assistant Secretaries of the Treasury, and met with the Justice Department, and they have been cordial meetings.

But the meetings have had one result, the same result you got this morning, which is that—and I will paraphrase what you just heard—we can see no changes in the process that we would be willing to consider.

We think there are better systems. We think there are better processes. And what we would ask for is a chance to have a summit or a working group, as you suggested, between law enforcement, the regulatory agencies, and the industry, with an open mind towards looking for improvements instead of a set of, well, this is the way we do it and we want to tell you why we do it that way.

We had those meetings, but we think some improvements are called for. Mr. Chairman, thank you for your leadership on this.

[The prepared statement of Mr. Bartlett can be found on page 51 of the appendix.]

Chairman WATT. Thank you for your testimony.

Ms. Hodge, you are recognized for 5 minutes.

STATEMENT OF MEGAN DAVIS HODGE, DIRECTOR, ANTI-MONEY LAUNDERING, RBC CENTURA BANK, ON BEHALF OF THE AMERICAN BANKERS ASSOCIATION

Ms. HODGE. Thank you. Mr. Chairman, and members of the subcommittee, I am Megan Davis Hodge, director of AML compliance and BSA officer for RBC Centura Bank, headquartered in Raleigh, North Carolina, appearing today on behalf of the American Bankers Association, the ABA.

ABA, its members and bankers from the boardroom to the teller line, have been steadfast partners in the effort to deter, detect, and defend against those who would abuse our financial system through fraud, money laundering, and terrorism financing.

Mr. Chairman, we appreciate that you have chosen to focus this hearing on better balancing law enforcement utility and regulatory requirements. We share your goal. Our mission is too important to squander resources on ineffective reporting. We need to give priority to the efforts that achieve the greatest bang for the buck and eliminate those that produce the least.

First, let me begin by briefly describing what banks must do to comply with suspicious activity reporting obligations, the cornerstone of the BSA.

First, to identify suspicious activity, the bank must undertake a detailed analysis for every geographic area, product, and customer category to identify that risk areas that merit additional scrutiny.

Second, we must monitor the ongoing banking activity of our customers to detect unusual activity. This detection could be triggered by an observant teller or by a manual or automated back office review of transaction records.

Once unusual transactions are flagged, an investigation is conducted that is tailored to the specific circumstances of the customer. These inquiries are sensitive and time-consuming.

After this detailed review, a SAR is filed if the bank believes that the customer's activity meets the reporting requirements. Through this process, the bank must comply with filing deadlines, transaction threshold levels, and report form requirements.

And finally, extensive records are required even if the decision is made to not file a SAR.

This is not the end of mandated compliance. Periodic summaries are given to senior management, and an independent audit function takes place to ensure that the SAR process is sound. Of course, none of this can take place without extensive and regularly updated employee training. As the more than 300-page interagency BSA examination manual demonstrates, there is not a bank operation, product, or customer beyond the reach of the SAR process.

What has this undertaking produced? It has produced a 600 percent increase in filings in the last 10 years, with no sign of abating, that from our perspective represents an excess of volume over value. Our conclusion is largely driven by two factors.

First, regulatory pressures promote the "when in doubt, file" mentality that inflates SAR volume out of proportion to the risk represented by the underlying conduct.

Second, in the absence of constructive feedback from law enforcement, banks identify an evolving array of fraud and other potentially serious crimes that expand the SAR universe regardless of the likelihood of action or interest by law enforcement.

Changes can be made to address these issues and improve SAR process efficiencies.

First, agencies can reduce the "when in doubt" defensive SAR filings by assuring examiners follow exam standards. It is the unwarranted substitution of examiner judgment for the bank's well-considered risk assessment that is causing these defensive filings. By abiding by the exam manual, which focuses on effective programs,

not quantitative outputs, fear of second-guessing will disappear and best judgment reporting will return.

Second, eliminate low-value SARs by better aligning SAR thresholds to prosecutorial standards and by leveraging specialized and accessible task forces to better pursue elusive scams.

Third, enhance SAR feedback by more specific tracking of the connection between SARs and the case results so that the reporting effort and law enforcement value are more visibly linked, as is done in other areas.

And finally, the time has come to eliminate currency transaction reports on seasoned business customers. ABA recognizes your strong leadership, Mr. Chairman, in pursing such initiative. Your efforts and those of your colleagues on the subcommittee were critical to passing H.R. 323, the Seasoned Customer Exemption Act of 2007, by voice vote in the full House.

Enactment of this legislation could be the most significant step to improve our anti-money laundering efforts by trading volume for value, not only with respect to CTRs but also with regard to SARs. If we are better able to remove some of the noise, both banks and law enforcement will be able to better focus resources on improving results.

Thank you, Mr. Chairman. I would be happy to answer any questions.

[The prepared statement of Ms. Hodge can be found on page 76 of the appendix.]

Chairman WATT. Thank you so much for your testimony.

Ms. Mroz, you are recognized for 5 minutes.

STATEMENT OF CAROLYN MROZ, PRESIDENT AND CEO, BAY-VANGUARD SAVINGS BANK, ON BEHALF OF AMERICA'S COMMUNITY BANKERS

Ms. MROZ. Chairman Watt, Ranking Member Miller, and members of the subcommittee, I am Carolyn Mroz, president and CEO of Bay-Vanguard Federal Savings Bank, a $134 million depository institution in Baltimore, Maryland. I am here today representing America's Community Bankers, ACB. I am a member of ACB's board of directors, and I serve on ACB's regulation and compliance committee.

BSA compliance requirements are always at the top of the list of the most burdensome regulatory requirements for community bankers. Community banks are being held responsible for the same BSA requirements as multinational banks despite differences in their businesses and fewer resources available. ACB supports the goals of these laws, but inconsistent interpretation and a lack of regulatory guidance has made it increasingly difficult for community banks to comply with anti-money laundering demands.

For example, in addition to serving as Bay-Vanguard's president and CEO, I am also our BSA compliance officer. We are a small bank with only 31 employees. Large community banks comply by employing a full-time senior level BSA officer, but I don't have that luxury.

Regardless of bank size, many additional employees have to work with the BSA officer to file the CTRs and SARs and to respond to Section 314(a) requests for information. The added payroll and ben-

efit costs, as well as specialized training and continuing education, are a significant expense for community banks.

Also, third party audits and legal advice for SARs determinations can cost a small bank well over $30,000 annually. These are real costs that have a great influence on the bank's ability to grow the business and serve the community. These burdens result in many lost opportunities.

Banks are providing much more data than law enforcement appears capable of using. While we are committed to providing the government with the necessary information to combat unlawful activities, a greater emphasis should be placed on the quality of the data rather than the quantity of the data.

We believe BSA requirements need to be modernized. For example, ACB believes that the BSA should be amended to provide an increase in the dollar value that triggers a CTR filing. The current $10,000 threshold was established in 1970. When adjusted for inflation, $30,000 in 1970 is equivalent to $53,000 today. Studies have shown that increasing the reporting threshold to $20,000 would decrease CTR filings by 57 percent, and increasing the threshold to $30,000 would decrease filings by 74 percent.

ACB also strongly urges the banking regulators, FinCEN and the Department of Justice, to work to help institutions identify activities that are truly suspicious and should be reported. Without additional guidance regarding what events should trigger an SAR, institutions will continue to face excessive compliance risk in an often zealous regulatory environment.

Financial institutions believe that the Federal Government has little understanding of the amount of time and resources that BSA compliance drains from an institution's ability to serve its community. What may seem like insignificant costs to law enforcement have very real business implications for community banks.

As an example, 314(a) requests for specific data every 2 weeks are very costly and generate few enforcement results. Banks should not be expected to report transactions to law enforcement or conduct business in an environment that expects compliance at any cost.

The time is now to review the BSA compliance requirements to ensure that the burden shouldered by the Nation's community banks is commensurate with a demonstrated benefit to law enforcement. Banks stand ready and willing to respond quickly and completely to legitimate requests from law enforcement agencies. But compliance burdens that simply generate mountains of data cannot be justified.

Thank you for your invitation to testify, and I would be glad to answer any questions.

[The prepared statement of Ms. Mroz can be found on page 110 of the appendix.]

Chairman WATT. Thank you for your testimony.

And Mr. McClain, you are recognized for 5 minutes.

STATEMENT OF SCOTT K. McCLAIN, DEPUTY GENERAL COUNSEL, FINANCIAL SERVICE CENTERS OF AMERICA

Mr. MCCLAIN. Thank you, Mr. Chairman, and members of the subcommittee. My name is Scott McClain, and I serve as deputy

general counsel to Financial Service Centers of America, also known as FiSCA. FiSCA is a national trade association representing over 6,000 neighborhood financial service providers throughout the United States.

FiSCA's membership is comprised of community-based financial institutions that serve millions of customers from all walks of life, including those with bank accounts as well as the unbanked. Our members provide a range of financial services, including check cashing, money transfers, and money order sales, among others.

Let me first say that FiSCA and its members are committed to the fight against money laundering and terrorist financing, and we have committed significant resources in this area. Ours is a regulated industry subject to many of the same types of reporting and recordkeeping requirements as banks and other depositories. As money service businesses, or MSBs, we are subject to rigorous compliance examinations by IRS agents. When viewed against the more traditional banking industry, our record of compliance is quite good.

SAR and CTR compliance requirements have resulted in substantial costs to the MSB industry in several key areas, including labor costs, information technology costs, professional service fees, and banking service charges. Banks that service MSBs have likewise experienced mounting compliance and monitoring costs, which are passed on to MSB customers in the form of increased service fees. Any analysis of the value of SAR and CTR information to law enforcement should take into account the costs to the MSB industry.

Since 9/11, there has been a tremendous increase in regulatory scrutiny of the financial services industry. Across the board, MSBs have responded to these pressures by defensive SAR filings. MSBs are persuaded that the key to avoiding penalties is to file reports on even marginally irregular activity. As a result, law enforcement agencies are deluged with SARs that may be largely useless.

Pressure towards defensive SAR filings emanates in many cases from field-level examiners who second guess decisions by compliance personnel. Examiners have been critical of MSBs who have not filed enough SARs. MSBs have also been cited for not reporting transactions that the MSB knew to be legitimate. As a result, MSBs are adopting a "when in doubt, fill out" philosophy.

To what extent are SARs valuable to law enforcement? What percentage of filed SARs lead to active investigation, and what percentage of those lead to criminal convictions? A critical analysis of these questions and the overall burden that SARs place on U.S. financial institutions is needed.

Additionally, FiSCA supports an increase in the reporting threshold of CTRs. As has been noted earlier today, the present $10,000 threshold was established in 1970. Since that time, the threshold has not been increased, and it has been rendered outdated due to inflation.

To a point made earlier by Mr. Bartlett of the Financial Services Roundtable, the post-9/11 atmosphere of fear has given rise to another indirect yet very costly burden to industry, particularly the MSB industry, and that is the termination of MSB bank accounts.

Depositories that service MSBs are faced with significant regulatory burdens, and are required to expend ever-greater resources in maintaining MSB compliance and monitoring systems. Due to this uncertain regulatory environment, many banks have opted to discontinue their check cashers and money transmitter customers.

It is critical to the interests of national security that transparency of MSB transactions be maintained by ensuring that MSBs remain part of the regulated financial community and continue to have access to depository services.

In conclusion, regulatory pressures and the lack of clear guidance in this area have resulted in a tremendous number of defensive SAR filings and duplicative CTR filings at tremendous cost to industry. The value of these reports should be evaluated, and the current reporting system and its cost to industry should be critically assessed.

Again, we thank you for the opportunity to present these views. I will be happy to address any questions that you may have. Thank you.

[The prepared statement of Mr. McClain can be found on page 87 of the appendix.]

Chairman WATT. Thank you for your testimony.

And Mr. Menzies, you are recognized for 5 minutes.

STATEMENT OF R. MICHAEL STEWART MENZIES, SR., PRESIDENT AND CEO, EASTON BANK & TRUST COMPANY, ON BEHALF OF THE INDEPENDENT COMMUNITY BANKERS OF AMERICA

Mr. MENZIES. Thank you, Chairman Watt, Ranking Member Miller, and distinguished members of the committee. As president and CEO of Easton Bank & Trust in Easton, Maryland, the home of the world-famous Waterfowl Festival, it is my honor to testify to you today as vice chairman of the—

Chairman WATT. World famous what festival?

Mr. MENZIES. Waterfowl Festival, during the first week of November every year. It is my honor to testify as vice chairman of the Independent Community Bankers of America and our 5,000 members, and to discuss the Bank Secrecy Act with you today, and to seek ways to prevent the Act from becoming form over substance.

We strongly urge Congress to recognize and identify the real costs that BSA requirements place on banks, especially community banks. Bankers across the country have identified this Act as one of the most burdensome of compliance acts in the regulatory body. Our focus should be based on finding risk-based approaches that balance the cost to the banking industry and our customers, and benefits to law enforcement.

To that end, we support a streamlined seasoned customer exemption from the CTR reports. In addition, law enforcement should clearly demonstrate the results produced from data collected. An open dialogue between law enforcement and the industry would help all of us focus our efforts on being more productive and effective. Fundamentally, specific feedback from law enforcement would help banks identify suspicious transactions. It would encourage us to understand that our efforts are truly worthwhile.

I am heartened to hear Director Baity say that he plans to take a fresh look at interaction with the banks and balancing cost versus regulations, especially understanding that the effort to modernize exemptions has been underway for almost 15 years now.

It is imperative that law enforcement understand the cost in terms of dollars, training, time, and regulations. And these costs are truly ultimately borne by our customers. We have 49 full-time employees, and more 8 percent of my staff is occupied with BSA compliance. Every employee receives 2 or 3 hours of BSA training every year. This training is costly and requires our employees to divert significant attention away from customer service.

In addition, we complete regular internal and external audits of BSA compliance. Quarterly internal audits require a minimum of 8 hours to complete. External audits cost us about $4,000 a year. When FinCEN asks my bank to search our records for data matches on suspicious individuals, each request requires at least 2 hours of research by three employees every 2 weeks. If a match is found, the time increases significantly.

Last year, as you pointed out before, Chairman Watt, over 17 million reports were filed. In the first 4½ months of 2007, our bank has filed more than double the number of SARs than last year. Although our CTR and SAR filings are automated, it still requires a minimum of 5 minutes to complete each CTR and up to 20 minutes to file an SAR.

Many institutions report the cost of using CTR exemptions outweighs any associated benefit. As a result, many institutions prefer not to use the exemptions and file the CTR in every case where it is over $10,000. Unlike these banks, we use the existing customer exemption, but we do it for only two customers. Without the exemption, we would have filed 65 more CTRs this year.

We applaud Ranking Member Bachus for taking the lead on this issue, and once again sending a seasoned customer exemption to the Senate in the form of H.R. 323, the Seasoned Customer CTR Exemption Act of 2007. We applaud this committee and the House for passing H.R. 323. We believe this bill is an important step to bringing the costs and the benefits of BSA reporting back into balance.

Specifically, H.R. 323 would streamline the exemption process and make it easier for banks to use. While this sounds like a small fix, it is important to community banks. It would result in substantial savings to our banks and increase the time employees can spend meeting our customers' financial needs.

The requirement to renew exemptions was one reason that banks chose not to use the exemptions. They fear—we fear—that missing the renewal or an unreported transaction would make us vulnerable to regulatory discipline and damage our reputation possibly in the community.

ICBA looks forward to working closely with Chairman Frank, Ranking Member Bachus, and members of this committee to find solutions that reduce the BSA compliance burden while still meeting the needs of law enforcement. Adoption of this important legislation is one step that will decrease the growing regulatory burden confronting all the banks of this Nation.

Thanks so much for your time.

[The prepared statement of Mr. Menzies can be found on page 97 of the appendix.]

Chairman WATT. I would like to thank all of you for your testimony. We have been advised that a series of votes may be imminent, so we want to try to get through the questioning session with this panel so that we don't have to detain you all here while we go and vote and come back. So perhaps we got carried away on the first panel, but we will try to restrict that this time.

Since Mr. Lynch has not asked any questions yet, I am going to recognize him first and then Mr. Miller. And I will go last, in case we run out of time before we get through everybody.

Mr. Lynch is recognized for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. I want to thank Mr. Miller as well for holding this hearing. I think it is an important one.

I wear two hats here this morning. I am also the chairman of the Task Force on Anti-Terrorist Financing, so these suspicious activity reports and the currency transaction reports are very important from an international standard as well.

I just came back from the Middle East. I met with the central bankers from Afghanistan, Jordan, and Turkey, and as well as our Treasury folks, FBI, FinCEN—I know they were in here a little earlier—trying to impose a system of transparency internationally to stop anti-terrorist financing.

And so I think the goal of this process here is to figure out, where is that balance where we can get enough information to feel confident that we are preventing terrorists from using the financial system to their end while not imposing undue burden on our banking system.

And I was encouraged as well at Mr. Baity's comments that we need to take a fresh look because some of these guidelines have been put in place many, many years ago and they need a fresh look.

But I have to admit, I come from this—because of the anti-terrorist task force, I come with some caution because I see us trying to regulate a global system where we are trying to institute transparency and encourage these other international banks, many of them in the Middle East, to give us suspicious activity reports.

I was in Ramallah recently. A lot of banking, a lot of economic activity, in Ramallah, in Jordan, in parts of the Middle East that we know there are some nefarious groups there that rely on illicit financing and money laundering to wage a terrorist war. And we are getting no SARs. We are getting no CTRs. And that has been difficult.

So while you are here saying we need less, I just think it sends the wrong message sometimes internationally. So we really do have to find that balance between getting enough information and instituting a standard that will be adopted internationally and will be effective internationally at the same time that we can allow banks to operate with less of a regulatory burden.

I would like to ask, though, and a number of people have mentioned the $10,000 trigger for suspicious activity reports or cash transaction reports. And that has been in place for a while. The International Convention on Anti-Terrorist Financing has that in it. In other words, a cash transaction over $10,000 should trigger

a report. But also, as little as $5,000 in a transaction can require a report if other factors are present.

Now, based on what you are dealing with right now, where do you think—and I will just ask the whole panel here—where do you think our numbers should be? What should trigger in a dollar amount or a factor consideration—what should trigger a suspicious activity report or a CTR today?

Mr. MENZIES. Congressman, I would be pleased to take a shot at that as a community banker.

Mr. LYNCH. Sure.

Mr. MENZIES. I don't have a dollar amount as a community banker. What I would like to see personally is substance over form. And I don't know that I can tell you that that occurs at $1,000 or $10,000 or $20,000 or $30,000. But I do believe I can tell you that we are reporting form in many cases and they are not of any substance at all.

Congressman Miller's description of the farmer was an experience that I had, where the farmer went to the Farm Bureau dinner and spoke with his brother and sold his brother his tractor for $12,000, and his brother said, I am going to pay you cash.

And he comes into the bank to deposit the cash, and he looks at his niece, who is the teller, and he says, how can I make this deposit so that you don't send it in to the IRS? Because I am told that you banks are sending all this stuff in to the IRS. And his niece now is involved in a structured transaction, and if she doesn't report an SAR, she has broken the law. And in my opinion, that is a great example of form over substance. So I think that the—

Mr. LYNCH. With all due respect, Mr. Menzies, that is a pretty highly specific case. I mean, not every businessperson out there has a niece who works as a teller. You are really—

Mr. MENZIES. It is a pretty unusual case. But Congressman, believe me, the public knows about the reporting process. This secret is not a secret. And it is not because the bankers are running around saying, listen, I am going to turn you in. The public knows about it.

And as Congressman Miller pointed out, there are a lot of people who are really concerned about these reports. And I am not—

Chairman WATT. The gentleman's time is expired, but I will allow each one of the witnesses to quickly—

Mr. LYNCH. Mr. Chairman, just one point and I will yield back.

Chairman WATT. Yes. Sure.

Mr. LYNCH. But that is the point. People are concerned. The terrorists are concerned. That is why they are avoiding the formal financial system, the formal banking system, is because they know. They won't use that system because they know a report will be filed. That is the point. That is why Mr. Haniyeh was confronted at Rafah Gate with $30 million in a suitcase, because he couldn't use the traditional banking system.

And that is what we want to do. We want to force them to use a hand courier system because there is a great risk, especially in the Middle East, to use that system. We don't want them in the standard banking system. And so while you see it as an encumbrance, there is also value in that, in squeezing the illicit money out of the system.

I yield back.

Chairman WATT. I thank the gentleman.

The gentleman from California is recognized for 5 minutes.

Mr. MILLER. Thank you very much. And I want to thank all of you for the private meeting we had to discuss this issue. We are never going to be able to touch on everything we dealt with in that meeting, and I want to thank you very much.

You heard the previous panel. What I am really convinced of is that we have a major failure to communicate here, and we have to address it. It is like one guy is going out to dinner with his family, and they have steak and lobster, and they say, that was a really good meal. The guy at the next table has to pay the bill.

And we need to understand how many of these SARs are beneficial, and how many are useless. I think a lot of it is going to deal with communication and how we go about doing it, and I just don't think that level of communication exists today.

The Bank Secrecy Act Advisory Group, I think, was intended to accomplish that. And obviously, it is not, based on information you gave me, the questions you gave me, the impact on your associations, your groups, your individual members, and yet when I talk to FinCEN out there and the FBI and law enforcement, their perspective and what they think they are generating from it.

But how successful do you think this advisory group has been, and how do you think we could enhance it in some way or modify it or change it or restructure it so that it would work? It would be beneficial for all the parties to get together and come up with something that people understand and your groups understand, and something that really generates information we need to have.

Why don't we start here and go right down.

Mr. BARTLETT. Mr. Miller, I didn't know it existed until this morning, if that gives you any indication.

Mr. MILLER. That is my point. It is communication with the industry. What I think this subcommittee could do would be to send staff to attend it, to create a balanced group with an open mind to look at the processes to determine how we can file suspicious activity reports in which some identifiable or some at least double-digit percentage of them are truly suspicious. But we are not getting an open mind or an open discussion at this point.

So if you would convene it and come to the meetings, and I know you would, with an open mind, perhaps we could get all sides to have an open mind in the discussion.

Ms. HODGE. The ABA believes that the BSAAG has been able to make some progress and can continue to work with continued focus on the issues as are being discussed today.

Mr. MILLER. Okay. I am going to give each of you a chance because we are not going to have time to go much farther today.

Ms. MROZ. I agree that I have never heard of that organization until today. And one of the concerns that I have is we are automatically linking CTRs and SARs, and I don't think they are necessarily linked at all. I do duplicate CTRs during the month for ma and pa customers of mine who are using cash. They bring in—you know, they are a convenience store and they sell cigarettes and gas. If they do that, they are over $10,000, probably, in 2 days.

And so I am not getting any information from those CTRs. My SAR investigations many times, most of the time, don't even come from a CTR.

Mr. MCCLAIN. Thank you. We believe that the BSAAG has been helpful and has resulted in some very good communication between the regulator and the industry. Additionally, some subcommittees were established on the BSAAG that resulted in some fruitful results.

Our concern would be at this point that there are not enough seats at the BSAAG and not all sections of industry are represented at the BSAAG at this point. There are just a limited number of seats open to the money service businesses industry at this point. There is a revolving process for being on the BSAAG, but again, we don't believe it is open enough for enough sectors of industry. Thank you.

Mr. MENZIES. I guess my own enhancement would be that they should write clear and measurable and understandable goals and objectives with a timeline to attain those goals and objectives.

Mr. MILLER. Well, Mr. Chairman, I think we need to look at the costs and the impact on the banks, and we also need to look at the benefit to counterterrorism and to money laundering and things that are going on in this country.

But we need to look at the structure. And there has to be some—there is an absolute disconnect today between law enforcement, FinCEN, and the industry who has to comply here. And we need to create a more transparent structure where people understand that—if you understood that there was tremendous benefit in what you were doing and the results that were coming out of it, you might look at some of this a little differently.

But I think from what we have talked about in the past, you are not sure that what you are doing is even being looked at, nor if there is any real benefit to most of what your compliance requires you to do. And I think that incumbent upon us to look at some way to make sure that that changes in the future.

And I thank you for your testimony, and I yield back.

Chairman WATT. I thank the gentleman. Let me recognize myself for just a few minutes to make comments and ask a couple of questions.

I think the thing that was most striking to me, as much complaints as we get from the financial sector about compliance with Sarbanes-Oxley and the cost of complying with Sarbanes-Oxley, is the statistic that is in Mr. Bartlett's testimony, that the cost of compliance with the Bank Secrecy Act is at least twice the cost of compliance with Sarbanes-Oxley. That is pretty dramatic since most of us on this committee are constantly hearing about the cost of Sarbanes-Oxley, and so there needs to be a look at how to understand this.

Now, let me just see if I can fix this in my own mind. Up to 1996, there was nothing like the suspicious activity report. You just had the currency transaction reports. Is it clear that a currency transaction report can be just done by technology? Do the community banks and independent bankers—do you have the technology that will just allow you to spit out a $10,000 cash transaction, and that is just a reporting function? Or is that adding burden to you?

And Mr. McClain, how does that play itself out in your world? I know the big banks can do it electronically, I presume. The big banks can do that electronically. What about community banks, independent banks, and the folks in your industry, Mr. McClain?

Mr. MCCLAIN. If I may, to two points on your question, Mr. Chairman. The cost, the labor costs, the man-hour costs that go ultimately into creation of the CTR forms, is quite substantial in the financial services industry. Virtually across the board, financial service companies' centers are required to either complete them manually—substantial man-hours go into that process—or they are required to adopt rather expensive data processing systems that allow them to automate some of that process. So there are cost factors in both elements of that.

Additionally, with respect to the e-filing of the CTR process through FinCEN, it is a very cumbersome process. It is designed for banks. It is not designed for smaller mom and pop operations such as a number of community financial service centers. So we believe that that particular process should be streamlined or looked at with regard to this industry, and that would certainly facilitate that process.

Chairman WATT. Mr. Menzies and Ms. Mroz, do your institutions—are they technologically able to comply with the CTR provisions? I am setting aside the SAR provisions now.

Mr. MENZIES. Mr. Chairman, we could if we were to invest in that software and in that technology. We have not, and—

Chairman WATT. What would that cost for a typical bank?

Mr. MENZIES. I don't know the exact cost. But I do know that it would be more expensive for us to go acquire the software than to continue to do it manually. One of the challenges is that when a CTR is presented, if the owner of the convenience store sends their clerk, Betty Lou, to make the deposit, then that information has to be captured. And you don't do that with software; you do it by the teller seeing that Betty Lou is making the deposit, not the owner of the convenience store. So there is some information that you just don't automate.

Chairman WATT. Ms. Mroz?

Ms. MROZ. We are not automated, either. And one of the other problems in addition is the aggregate. If they do two transactions in one day and neither one of them are over $10,000, we have a human being who is tracking those transactions. We get a large transaction report of anything over $5,000, and we try and match up. Someone is physically every day checking that report to make sure that there aren't multiple transactions from any one customer that also exceeds $10,000.

And again, money is driving the bus. We can't afford the software. I have heard quotes anywhere from $30,000 to $100,000 for that software. And for a community bank, that is just—we can't afford it.

Chairman WATT. Ms. Hodge?

Ms. HODGE. Mr. Chairman, if I may, certainly larger banks oftentimes have invested the financial resources in order to facilitate a more automated filing process. But they are still not immune from the situations that you have just heard described that do require manual intervention, sometimes by the teller itself as they

are conducting the activity to obtain the information accurately on the person conducting the transaction, and then sometimes in the back office trying to piece together the aggregated information or perhaps correct errors that were made on behalf of the teller.

Chairman WATT. Well, obviously, there are a myriad of other questions that we have not gotten to today. So I will just note that some members may have additional questions for this panel also and may wish to submit them in writing. And 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. And we would ask you, if that occurs, to respond promptly.

We thank the witnesses for being here. I don't think you want to wait for what appears to be about 45 minutes to have us come back to continue this questioning. I hope you will find it preferable to answer additional questions in writing. But we want to thank you for being here. We think it has been an effective first hearing on this issue, and the subcommittee will stand adjourned.

[Whereupon, at 11:01 a.m., the hearing was adjourned.]

A P P E N D I X

May 10, 2007

OPENING STATEMENT OF
CHAIRMAN MELVIN L. WATT

SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS

HEARING ON "SUSPICIOUS ACTIVITY AND CURRENCY TRANSACTION REPORTS: BALANCING LAW ENFORCEMENT UTILITY AND REGULATORY REQUIREMENTS"

THURSDAY, MAY 10, 2007

We meet this morning to explore Suspicious Activity and Currency Transaction Reports which are required under the Bank Secrecy Act of 1970 (BSA). This is the first in a series of hearings to explore SARs and CTRs, the real-life experiences of financial institutions in complying with SARs and CTRs and these reports' utility to law enforcement.

First, I want to welcome all of the witnesses and thank them for taking the time today to appear before this Subcommittee on this very important issue. I want to say a special hello to Megan Hodge who is the Director of Anti-Money Laundering for RBC Centura Bank, from my home state of North Carolina.

After 9/11, there has been increased focus on rooting out financial crimes including terrorist financing and money laundering, and rightly so. As a result of this increased emphasis on detecting financial crimes, financial institutions have had to assume a much larger role, becoming full partners with law enforcement.

SAR and CTR reporting is one very important way that the financial industry has partnered with law enforcement. Today, there are millions of SARs and CTRs filed annually with the Financial Crimes Enforcement Network (FinCEN). Deputy Director Baity of FinCEN is here this morning, and we look forward to his testimony.

In this hearing, we hope to fully explore what reports are useful and which ones are not so useful. We know that under the BSA, financial institutions must report all

transactions of $10,000 or more on a Currency Transaction Report and report suspicious activity on a Suspicious Activity Report. What we do not yet fully understand is how financial institutions, including depository institutions, money services businesses and others actually comply with SAR and CTR reporting, and if the guidance given to them by regulators is appropriate and effective.

We also want to explore the practical effects of BSA reporting. How do financial institutions detect suspicious activity - - through the use of automated computer systems, "human intelligence" or some combination? Are there increased costs to financial institutions of BSA compliance, and are those costs passed on to consumers? How do financial institutions train their staff to recognize and report suspicious activity? Is better guidance needed?

We also want to explore the utility of increased SAR and CTR filings to law enforcement. Is law enforcement receiving robust, useful data from FinCEN and financial institutions? Are there changes that law enforcement would like to see in FinCEN guidance to financial institutions or in the SAR form itself?

The point of this hearing is to elicit information. Understanding the full scope of BSA reporting, particularly SARs and CTRs is a bi-partisan objective. We do not have any pre-conceived ideas as to the utility of SARs and CTRs, or have in mind any particular legislative action. Rather, we are here to learn and benefit from the witnesses' collective knowledge and experience with BSA reporting.

We all must recognize that increased BSA reporting does have some costs: financial institutions spend millions of dollars a year in BSA compliance, some of which undoubtedly gets passed onto consumers. Americans' privacy and civil liberties must be balanced with assisting law enforcement. We all seek to equip law enforcement with the tools they need to help keep America safe, especially after 9/11. We want the information they receive, however, to be robust and effective.

Statement of Representative Gary G. Miller
Subcommittee on Oversight and Investigations
Committee on Financial Services
Hearing Preparation, "Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements."

May 10, 2007

Today, the Subcommittee on Oversight and Investigations meets to consider the usefulness of data collected by financial institutions pursuant to the Bank Secrecy Act (BSA) compared to the costs and burdens of compliance. I commend Chairman Watt for convening this hearing today and I look forward to working with him to find a reasonable balance between the information needs of our nation's law enforcement authorities to combat financial crime and terrorist financing and the burdens placed on financial institutions to provide such information.

The BSA was enacted in order to prevent financial institutions from being used to hide or transfer money derived from or intended to finance criminal activity. The law and regulations supporting BSA require the creation of a paper trail for certain high dollar or suspicious transactions. The Suspicious Activity Reports and Currency Transaction Reports that are required to be filed by financial institutions are utilized by law enforcement to investigate money laundering schemes and other illegal activities. This effort, if undertaken reasonably, can be for the benefit of both the financial industry and our nation.

I think everyone in this room can agree that it is of utmost importance to do what we can to keep our country safe from terrorism and to keep money launderers and other criminals from using our financial system to further their unlawful activities. The reason we are here today is that we have asked financial institutions to bear the burdens of reporting information to law enforcement that could potentially help in this effort. We do not pay for them to do this and there is clearly a cost of reporting in time and resources. Instead of compensation for compliance, we threaten penalties for non-compliance. Of course, like anything else the costs of compliance are ultimately borne by consumers in the form of more expensive banking services and credit options.

It is our responsibility to financial institutions, and ultimately to our constituents, that as we work to detect criminal activity through our financial system, we also work to ensure that what we are requiring to be reported is necessary and valuable. We must also be careful that our requests for information are not unreasonably burdensome.

The hearing today will explore how close we are to achieving this important balance. Both sides have made convincing arguments in their written testimony, indicating to me that we are not quite there yet. Banks are willing to report the information – they just want more understanding built into the system, more certainty about what they should and should not file, and more uniformity in regulation. And they want the filing requirements to be realistic and based on an assessment of actual risks. Law enforcement want to have as much information as possible to fight financial crimes and cut off terrorist financing. Financial information has been shown to be an important evidentiary tool to help stop terrorists before they strike and to detect

criminal activity in our society. The fear is that if we change what is required to alleviate the burden on financial institutions we run the risk of losing information that is critical to our security. I agree with both sides and believe there is validity to each position. But, I also believe that the goals of law enforcement and financial institutions are not incompatible. As long as we work together, we can find the right balance.

I supported efforts, led by full committee Ranking Member Bachus, to create a seasoned customer exemption for the filing of CTRs because I thought it was a good step in achieving such a balance. This legislation would preserve the integrity of our law enforcement efforts while at the same time reducing a reporting burden on banks. If an exempted seasoned customer did something suspicious, then law enforcement would still know about it because the financial institution would file a Suspicious Activity Report. Otherwise, if the seasoned customer's behavior never changed, then there would be no need to ask a financial institution to file a CTR every time that small business made a cash deposit. We are told by banks that the current CTR exemption process is underutilized because it is more costly and time consuming to apply for the exemption than to file the CTR. I think the seasoned customer exemption will address some of the banks' concerns with the current exemption system. I am glad the House acted swiftly this year to pass H.R. 323 because this is a simple step we can take to address the strain on financial institutions' resources by having to file unnecessary CTRs without compromising law enforcement investigations.

The bottom line is that we need to come together to find workable solutions to improve the effectiveness of the current system. We are told that the information reported by financial institutions is extremely valuable to law enforcement. I do not support hampering their efforts to keep our country safe. But I also do not support the status quo, where there is inconsistent regulation of BSA requirements and where banks feel the need to "defensively file" reports to protect themselves. We can not tolerate a system that is inconsistently applied and creates a sense of trepidation among financial institutions rather than a sense of duty and purpose. Financial institutions are an important part of our efforts to fight crime and our policies toward them should treat them as such.

On FinCEN's website, it states, "Working together is critical in succeeding against today's criminals. No organization, no agency, no financial institution can do it alone." I am pleased that FinCEN recognizes the importance of viewing financial institutions as a partner in their efforts to combat money laundering and terrorist financing. Our purpose is clear: we must ensure that this partnership is reflected in policy, regulation and practice.

I look forward to hearing from the witnesses today. I hope this hearing will continue the dialogue that resulted in House passage of H.R. 323.

STATEMENT OF WILLIAM F. BAITY
DEPUTY DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK
UNITED STATES DEPARTMENT OF THE TREASURY

BEFORE THE
HOUSE FINANCIAL SERVICES SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

MAY 10, 2007

Chairman Watt, Ranking Member Miller and distinguished members of the Subcommittee, on behalf of our Director and the men and women of the Financial Crimes Enforcement Network (FinCEN), we appreciate this opportunity to appear before you today to discuss the utility of information provided by financial institutions in accordance with the provisions of the Bank Secrecy Act (BSA). As the administrator of the BSA, FinCEN continually strives to maintain the proper balance between the reporting requirements imposed upon the financial services industry, and the need to ensure an unimpeded flow of important information to law enforcement officials. We take this responsibility very seriously, and we look forward to working with the Members of this Subcommittee in our united fight to safeguard the U.S. financial system against all types of illicit financial activities.

I am also honored to appear today with Salvador Hernandez, Deputy Assistant Director for the Criminal Investigative Division of the Federal Bureau of Investigations (FBI). Our partnership with the FBI, as well as other law enforcement agencies, allows for a seamless flow and effective utilization of BSA information in our united fight against terrorist financing and money laundering.

As you know, FinCEN's mission is to safeguard the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit financial activity. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Administering the Bank Secrecy Act - the United States' primary anti-money laundering/counter-terrorist financing regulatory regime;

- Supporting law enforcement, intelligence, and regulatory agencies through the sharing and analysis of financial intelligence; and
- Building global cooperation and technical expertise among financial intelligence units throughout the world.

To accomplish these activities, FinCEN employs a team comprised of approximately 300 dedicated federal employees, including analysts, regulatory specialists, international specialists, technology experts, administrators, managers, and Federal agents who fall within one of the following mission areas at FinCEN:

- **Regulatory Policy and Programs** - FinCEN issues regulations, regulatory rulings, and interpretive guidance; assists state and federal regulatory agencies to consistently apply BSA compliance standards in their examination of financial institutions; and takes enforcement action against financial institutions that demonstrate systemic non-compliance. These activities span the breadth of the financial services industries, including – but not limited to – banks and other depository institutions; money services businesses; securities broker-dealers; futures commission merchants and introducing brokers in securities; dealers in precious metals, stones, or jewels; insurance companies; and casinos.

- **Analysis and Law Enforcement Support** – FinCEN provides federal, state, and local law enforcement and regulatory authorities with different methods of direct access to reports financial institutions submit pursuant to the BSA. FinCEN also combines BSA data with other sources of information to produce analytic products supporting the needs of law enforcement, intelligence, regulatory, and other financial intelligence unit customers. Products range in complexity from traditional subject-related research to more advanced analytic work including geographic assessments of money laundering threats. It is this latter type of analytical work that we believe is where FinCEN can and should focus its' limited resources to have the greatest impact. I will discuss this in more detail later in my statement.

- **International Cooperation** – FinCEN is one of 100 recognized national financial intelligence units around the globe that collectively constitute the Egmont Group. FinCEN plays a lead role in fostering international efforts to combat money laundering and terrorist financing among these financial intelligence units, focusing our efforts on intensifying international cooperation and collaboration, and promoting international best practices to maximize information sharing.

ADMINISTERING THE BSA

The BSA is the nation's first and most comprehensive federal anti-money laundering statute. Since it was enacted in 1970, the BSA has been amended on numerous occasions, most recently by the USA PATRIOT Act. Essentially the BSA is a recordkeeping and reporting statute. The BSA authorizes the Secretary of the Treasury to issue regulations requiring identified types of financial institutions to submit certain information, to maintain certain records, to implement appropriate anti-money laundering programs. Under the BSA, these efforts are focused on obtaining the information that has a high degree of usefulness in criminal, tax, regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters. The BSA data received through Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), and other forms have proved to be highly valuable to our law enforcement customers, who use the information on a daily basis as they work to investigate, uncover, and disrupt the vast networks of money launderers, terrorist financiers and other criminals. In addition to obtaining information for law enforcement, BSA programs help financial institutions protect themselves, and subsequently the U.S. financial system, from abuse from criminal actors.

Part of FinCEN's mission is to push for the appropriate level of transparency in the U.S. financial system so that money laundering, terrorist financing and other economic crime can be deterred, detected, investigated, and prosecuted. Our ability to tie together and integrate our regulatory, international, and law enforcement efforts assists us to achieve consistency across our regulatory regime.

The efficient administration of the BSA is much more than simply issuing regulations. To work, it requires an ongoing partnership between the government and private sector, which is critical in order to achieve the goals of the system. One way to make this partnership work is the ongoing effort of the Bank Secrecy Act Advisory Group (BSAAG). The BSAAG includes membership from a diverse group of the types of financial institutions subject to the BSA, law enforcement, federal and state, regulators, federal and state that come together twice a year with FinCEN to discuss ways in which the BSA can be administered more efficiently. These discussions are open, frank and comprehensive. Within the BSAAG there are formulated sub-committees to address specific issues. They include ways to improve exemption programs for the filing of CTRs, the registration processes for money service businesses (MSBs), general issues associated with SAR forms, examination concerns, privacy issues, and the SAR Activity Review, which provides bi-annual SAR statistics. FinCEN will continue to explore ways in which financial institutions can take advantage of the exemption processes.

We have partnered with the federal and state regulators to encourage financial institutions subject to the BSA to develop risk-based anti-money laundering programs tailored to their businesses, and provide guidance in this regard. Such programs include the development and implementation of policies, procedures, and internal controls needed to address financial crime, including money laundering, terrorist financing, and other risks posed by that financial institution's products, geographic locations served, and customer base.

We have learned that in order for this system to work, the government must provide guidance and feedback to the industry in ways that support their understanding of potential vulnerabilities, effective ways to address those vulnerabilities and the benefits derived from information reported by them. The risk-based nature of the regulatory scheme also recognizes that financial institutions are in the best position to design anti-money laundering/counter-terrorist financing programs that address the specific risks that they face. In other words, the success of this regime depends upon the government and financial institutions acting in true partnership – each committed to the goal of taking reasonable steps to ensure that the financial system is protected from criminals and terrorists to the greatest extent possible through the development of appropriate programs and the sharing and dissemination of information.

Ensuring that we strike the right balance between the cost and benefit of this regulatory regime is one of FinCEN's central responsibilities. Accordingly, it is vital that we continue to examine how we can more effectively tailor this regime to minimize the costs borne by financial institutions while at the same time ensuring that the law enforcement, intelligence, and regulatory communities receive the information they need.

SUBMISSION OF BSA REPORTS

In accordance with the committee's request, we have included relevant statistics regarding the submission of reports pursuant to the BSA. The BSA's record keeping and reporting requirements increase transparency in the financial system and help to create a financial "paper trail" that law enforcement and intelligence agencies use to track criminals, their activities, and their assets.

Currently the forms for submitting information pursuant to the BSA include:

- Currency Transaction Reports (CTR) - currency transactions of $10,000 or more or structuring

- Currency Transaction Reports by Casinos (CTR-C)

- Currency Transaction Reports by Casinos – Nevada[1]
- Suspicious Activity Report (SAR) - depository institutions
- Suspicious Activity Report by Casinos and Card Clubs (SAR-C)
- Suspicious Activity Report by a Money Service Business (SAR-MSB)
- Suspicious Activity Report by Securities and Futures Industries (SAR-SF)
- Suspicious Activity Report by Casinos and Card Clubs (SAR-C)
- Report of International Transportation of Currency or Monetary Instruments (CMIR)[2]
- Report of Foreign Bank and Financial Accounts (FBAR)
- Registration of Money Services Business
- Report of Cash Payments over $10,000 Received in a Trade or Business (Form 8300)

Preliminary data received from the Internal Revenue Service's Enterprise Computing Center in Detroit, which receives and processes BSA reports on behalf of FinCEN shows the number of BSA reports filed in Fiscal Year 2006 rose to approximately 17.6 million, compared to about 15.6 million in Fiscal Year 2005. The reports filed most often are:

1. **CTRs** all types - 15,994,484 – which are filed in connection with cash deposits, withdrawals, exchanges of currency, or other payments or transfers by, through, or to a financial institution involving a transaction *(or multiple transactions by or on behalf of the same person)* in currency exceeding $10,000.

2. **SARs** - all covered institutions - 1,049,149 - which are filed in connection with transactions that financial institutions know, suspect, or have reason to believe, may be related to illicit activity. These reports are especially useful to law enforcement and other relevant agencies because they reflect activity considered problematic or unusual by financial institutions, casinos, MSBs, and the securities industry.

---

[1] Nevada will be assimilated into the national system of BSA administration effective July 1, 2007.
[2] Collected by U.S. Customs and Border Protection.

In FY2006, approximately 43% of the CTRs viewed by Gateway users were identified as "of interest" to users at the time they were viewed. A review of closed FinCEN investigative cases for FY 2006 revealed CTRs were included in almost a third of the total cases. Moreover, nearly half of the cases completed for domestic customers and almost a quarter of the cases completed for foreign partners included CTRs.

BSA DIRECT

Given the magnitude of reporting, we believe it is incumbent on FinCEN as the administrator to examine how this data is collected. BSA Direct is an overall umbrella project with several components, including: electronic filing, retrieval and sharing, and secure access. It is meant to be a system to handling the data received, from submission to analysis to dissemination to our various stakeholders.

The electronic filing and secure access components of BSA Direct have been operational for a number of years. The retrieval and sharing development began conceptually in September of 2003, with a contract awarded on June 30, 2004. The retrieval and sharing (R&S) component of BSA Direct was, in part, aimed at improving authorized users' access and ability to analyze the BSA data. It was designed to apply data warehousing technology to cleanse and structure the data in a single, integrated, secure web-based environment, and provide sophisticated business intelligence and other analytical tools in a user-friendly web portal. Under this design, law enforcement and regulatory agencies would gain easier, faster data access and enhanced ability to query and analyze the BSA data - improvements that were expected to lead to increased use of the BSA data and enhancements of its utility.

On March 15, 2006, FinCEN notified Congress of its intention to issue a temporary 90-day "stop-work" order on this project. This action was necessary due to the project's inability to meet performance milestones. An assessment team, comprised of management, analysts, technology specialists, and independent consultants, was created shortly after the issuance of the stop-work order to assess and refine core requirements for BSA information retrieval, dissemination, sharing, and analysis; to determine whether this component of BSA Direct could be salvaged and/or leveraged by other alternatives; and to define the best path to ensure business continuity.

On July 10, 2006, the assessment team reported its findings and concluded that BSA Direct R&S was a partially built system that integrated a number of best-in-class products that did not, in its present state, function well together. As a result, the system could not be deployed to any of FinCEN's users in the short term. Moreover, FinCEN, the contractor, and our external consultants could not

definitively predict how close the system was to meeting the envisioned requirements or the time, resources, and risks involved in completing the system.

Based on these findings, the assessment team recommended that FinCEN terminate the existing contract, assess immediate needs, and plan for new capabilities. Based on the underlying information and analysis, FinCEN supported this recommendation and, therefore, on July 13, 2006, terminated the BSA Direct R&S contract.

FinCEN is undergoing a bureau-wide IT management analysis and planning effort re-planning effort for BSA Direct R&S to address strategic, technical, and resource planning issues with all of its IT systems, as well as stakeholder analysis, in order to identify a path forward. In addition, we will continue our efforts with the Internal Revenue Service to implement WebCBRS as a means of meeting internal and customer needs for BSA data query.

UTILITY OF THE INFORMATION SUBMITTED PURSANT TO THE BSA

FinCEN's Analysis and Liaison Division is responsible for analyzing BSA data and other information to produce analytic products supporting domestic law enforcement, intelligence, and foreign financial intelligence unit (FIU) customers. In addition, this division acts as a liaison with domestic law enforcement agencies and with counterpart FIUs in other countries. They also provide direct secure access to BSA data for domestic law enforcement and regulatory agencies. Their analytic products range in complexity from traditional suspect-related reports to policy-level assessments of financial crime threats. Consistent with FinCEN's strategic plan, analytic resources are being transitioned toward analysis that focuses increasingly on FinCEN's unique skills and knowledge of BSA data.

In Fiscal Year 2006, FinCEN produced 1,284 "Basic" analytical products which consist of suspect-based database queries and reports requiring relatively straightforward interpretation of findings. By contrast, FinCEN produced 176 "Complex" analytical products. These products include synthesis of data from multiple sources, interpretation of findings and recommendations for action and/or policy. Examples are geographic threat assessments, analyses of money laundering/illicit financing methodologies, analytic support for major law enforcement investigations, and analysis of BSA compliance patterns. Listed below are a few examples of "complex" analytic products produced by FinCEN:

Mortgage Loan Fraud - FinCEN's Office of Regulatory Analysis conducted this assessment to identify any trends or patterns that may be ascertained from an analysis of SARs regarding suspected mortgage loan fraud. Analysts searched the BSA database for SARs from depository institutions filed between April 1, 1996 and March 31, 2006 that contained "Mortgage Loan Fraud" as a

characterization of suspicious activity. The search retrieved 82,851 reports, which were examined to discern the trends and patterns revealed in this assessment. A random sample of 1,054 narratives was reviewed for additional analysis and revealed - among other trends addressed in this report - a sharp increase in the number of SARs reporting mortgage loan fraud beginning in 2002. We have received substantial positive feedback from the law enforcement, regulatory and financial communities on this report.

Domestic Shell Companies - In response to concerns raised by law enforcement, regulators, and financial institutions regarding the lack of transparency associated with the formation of shell companies, FinCEN prepared an internal report in 2005 on the role of domestic shell companies (and particularly LLCs) in financial crime and money laundering. An updated version of this report was publicly released in November 2006, along with an advisory to financial institutions reminding them of the importance of identifying, assessing and managing the potential risks associated with providing financial services to shell companies. FinCEN found that abuse of shell companies for illicit financial purposes is not limited to activity within the U.S. A review of SAR data indicates that suspected shell companies incorporated or organized in the U.S. have moved billions of dollars globally from bank accounts located in foreign countries, such as Russia and Latvia.

Domestic Geographic Threat Assessments – In response to requests from the Texas Department of Public Safety and the Arizona Attorney General's Office, FinCEN prepared three major assessments of financial activity along the U.S. southwest border to support state and federal drug and cash interdiction efforts. These three assessments, based on analysis of all BSA reports filed in border countries, identified potential money laundering hotspots and significant changes in financial activity to help states and federal authorities allocate resources on the southwest border.

To understand the overall value of BSA reports, it is important to obtain an understanding of how they collectively work in the detection/prevention of financial crime. For example, CTRs generally capture a transaction at a point in time. If a customer makes a deposit in cash for $12,000 at his bank, within fifteen days of the transaction the bank files a CTR. The CTR provides law enforcement information that can be invaluable in an investigation including the following: (1) who benefited from the transaction; (2) who conducted the transaction; (3) the dollar amount of the transaction; (4) how the transaction was conducted *(in person, ATM, night deposit, etc)*; (5) the purpose of the transaction *(deposit, withdrawal, purchase of monetary instruments, etc.)*; (6) what account numbers are affected; (7) where the transaction took place; and (8) when the transaction occurred.

Financial institutions file Suspicious Activity Reports (SARs) after a

subjective review of numerous variables, including the appearance of avoiding other filing requirements. While this subjective review can often lead to a more fulsome provision of facts to law enforcement, it works best in conjunction the availability of the more objective reporting requirements.

Both SARs and CTRs and work in conjunction to protect the US financial system. Although difficult to quantify, there is arguably some deterrence value associated with CTRs. Nearly half (48%) of all SARs filed relate to structuring/BSA/money laundering. Structuring is the process a person performs to avoid a CTR and is illegal. The CTR, therefore, serves as a benchmark for financial institutions and for those engaged in illegal activity. Much of the SAR data law enforcement employs in protecting the U.S. financial system derives from those who attempt to avoid a CTR. FinCEN continues to view CTRs useful in their own right because of the paper trail they create which we analyze. Moreover, a well balanced and managed CTR regime also provides a means of deterrence for illicit financial actors.

In conclusion, Mr. Chairman, we are grateful for your leadership and that of the other Members of this Subcommittee on these issues, and we stand ready to assist in your continuing efforts to ensure the safety and soundness of our financial system. Thank you for the opportunity to appear before you today. I look forward to any questions you have regarding my testimony.

Testimony of

Mr. Steve Bartlett

On Behalf of

The Financial Services Roundtable

To The

Subcommittee on Oversight and Investigations

Hearing on Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements

May 10, 2007

Introduction

Good morning, Chairman Watt, Ranking Member Miller, and Members of the Oversight Subcommittee. My name is Steve Bartlett, and I am President and Chief Executive Officer of The Financial Services Roundtable.

The Roundtable represents 100 of the nation's largest integrated financial services companies. Our members provide banking, insurance and investment products and services to millions of American consumers. Roundtable member companies account for $65.8 trillion in managed assets, $1 trillion in revenue, and 2.4 million jobs.

I would like to begin by thanking the members of the Subcommittee and Chairman Watt, in particular, for holding this hearing. While, the Roundtable unequivocally supports the need to forcefully and effectively combat terrorist financing and money laundering activities, we believe that the current BSA/AML reporting system could be improved to more effectively combat money laundering, assist law enforcement, and improve the ability of our legitimate customers to access the financial services system. Our member companies tell us Suspicious Activity Reports ("SARs") and Currency Transaction Reports ("CTRs") filings continue to rise, and most of these filings have little direct connection to money laundering or terrorist financing investigations. Consider, for example, the dramatic increase in SAR filings in recent years. In 1996, there

were 62,473 SARs filed. By 2005, almost 1 million SARs were filed.[1] Many of these reports are never examined. The Roundtable believes that BSA/AML compliance should be focused on the effectiveness of filings, not the number of filings. It is results that count, not inputs.

One Roundtable member company recently hired 200 new FTEs just to keep pace with CTR filings. Another Roundtable company, M&T Bank, which is one of the best managed companies in America, devoted almost four pages to the matter in its recent annual report. M&T estimates the annual recurring direct expense of AML compliance is approximately $3.3 million—almost twice the amount spent on Sarbanes-Oxley compliance. A study by the Institute for International Economics estimates that the BSA/AML compliance costs for financial institutions equal approximately $7 billion a year. That study further estimates that consumers bear an additional $1 billion as a result of the current BSA/AML compliance regime.[2]

1. See FenCen's SAR Activity Reports at www.fincen.gov

2. See American Banker Article, *"Vague Guidance Still Invites Defensive SARs"* by Reginald J. Brown and Stephen R. Heifetz (January 6, 2006)

The members of the Financial Services Roundtable wish to work with law enforcement and regulators to assess the usefulness and value of the large volume of SARs and CTRs in combating money laundering. Toward that end, we--

- Propose the creation of a Working Group to assess and improve the BSA/AML reporting system;
- Urge regulators to reduce ad-hoc BSA/AML supervisory practices and address Alien Tort Act/Anti-Terrorism Act Law suits; and
- Urge Congress to enact H.R. 323 the Seasoned Customer CTR Exemption Act of 2007.
- If the first three proposals are not addressed, then we recommend that the Treasury Department codify the good faith standard in the anti-money laundering examination manual in order to reduce defensive SAR filings.

Working Group to Improve BSA/AML Reporting System

The Roundtable believes that the opportunity exists to make our current BSA/AML reporting system more effective in the fight against money laundering and terrorist financing. This goal can be greatly facilitated by the creation of a BSA/AML Working Group composed of federal banking regulators, representatives of the law enforcement community, and financial institutions.

Such a Group should be charged with assessing the effectiveness of current BSA/AML reporting requirements and proposing appropriate reforms to Congress.

I urge Congress to establish this Group and to set a time-table to analyze the effectiveness of the anti-money laundering and anti-terrorist financing requirements applicable to financial services firms and report its findings to Congress. Such an assessment should not be seen as an attempt to reduce the BSA compliance burden on financial services firms. The Roundtable is committed to the goals of the BSA. However, many of the existing requirements have been in place for years, and some were imposed in response to specific developments. In addition, since the enactment of the BSA in 1970, there have been significant advances in business practices and technology, and some of the requirements may not utilize the cutting edge of existing practices and technology.

An assessment of the effectiveness of the existing requirements and their implementation would help to ensure that the requirements applicable to financial services firms do, in practice, deter financial crimes and lead to the prosecution of those crimes. We believe the assessment should:

1. Propose the creation of a Working Group to assess and improve the BSA/AML reporting system:
    - Conduct comprehensive review of the needs of law enforcement's money laundering reporting needs,

- Focus on the effectiveness and the value of the information requested by law enforcement and require better explanation for use of the information obtained by law enforcement,
- Evaluate the cost-benefit of the information collected by law enforcement; and
- Access the practicability of law enforcement requesting information related to money laundering directly from institutions.

2. Devise improvements to current system to better accomplish BSA reporting requirements:
   - Develop risks-base principles for reporting suspicious activities,
   - Narrow the scope for reporting suspicious activities by financial institutions,
   - Improve the use of technology in BSA reporting, and
   - Increase the reliance on "due diligence" rules for BSA reporting.

Ad-hoc Supervisory BSA/AML Practices & Alien Tort Act/Alien Terrorism Act Law Suits

A. Recently, the federal banking agencies issued a joint BSA/AML supervisory manual. The release of this manual was an extremely useful step in establishing uniform BSA/AML supervisory practices. However, Roundtable member companies still report that the supervisory environment remains somewhat ad hoc. We understand that regulators continue to develop compliance standards through the examination process on an institution-by-institution basis. For example, one Roundtable member company has reported that examiners, using so-called "due diligence" rules, are second guessing the institution's BSA/AML policies, and forcing the institution to retroactively close accounts that involve small dollar amount transactions. This ad-hoc approach results in inconsistent regulatory standards and inconsistent information to regulators and law enforcement. It also adds compliance costs to the industry, some of which are ultimately passed along to consumers. We believe that regulatory standards should be clear and consistent for the entire industry, and developed in an open and transparent manner.

B. The Roundtable is also concerned about potential litigation issues surrounding BSA/AML compliance under the Alien Tort Act & Anti-Terrorism Act. To date, this act has been used to sue three foreign banks with U.S.

branches. The banks are being sued in connection with their customers in non-US branches that have engaged in transactions outside the United States. These banks are complying with their own country laws. One troubling aspect of these cases is that the judges presiding over these cases have suggested in their decisions that banks may be required to consult terrorist lists outside of their home jurisdiction.

Good Faith Standard

Again, if the Roundtable first three aforementioned proposals are not addressed then we recommend that the Treasury Department codify the "good faith" standard that is contained in the Anti-Money Laundering Examination Manual. We believe that codifying the "good faith" standard would help to reduce defensive SAR filings and permit law enforcement agencies to focus valuable resources on serious crimes.

That standard reads as follows:

> In those instances where a bank has an established SAR decision-making process, has followed existing policies, procedures, and processes and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

This standard reflects the inherently subjective nature of SAR filings and the impossibility of detecting and reporting all illicit transactions that flow through an institution. While the standard is designed to focus attention on policy, procedures and processes, it has not deterred defensive filings. It has not done so because it is an "informal" statement of policy, rather than a "formal" regulatory standard. By adopting the standard as a regulation, Treasury would send a strong signal to all financial services firms that the focus of SAR compliance is on policies, procedures and processes, not individual filing decisions. This would reduce defensive filings and permit law enforcement agencies to focus their resources on serious crimes

Exemption for Seasoned Customers

We wish to thank the members of the Financial Services Committee and your House colleagues for approving H.R. 323, the "Seasoned Customer CTR Exemption Act of 2007." This bill would create a filing exemption for transactions with long standing and well known customers. It's an appropriate modification to the CTR filing requirement and will not diminish anti-money laundering enforcement.

Conclusion

In conclusion, the Roundtable appreciates the efforts of the Subcommittee in bringing attention to our BSA/AML regulatory compliance system. I wish to state again that the Roundtable supports and appreciates the work of the regulators and law enforcement.

Yet, we believe the current compliance system can be improved following a thorough assessment. A Working Group to assess and improve BSA/AML reporting is needed.

Thank you.

Attachments

Lawsuits May Boost Banks' Anti-Laundering Burden

American Banker

Wednesday, April 4, 2007

By Cheyenne Hopkins

WASHINGTON — A number of class actions in New York have the potential to redefine how far banks have to go to vet customers for potential ties to terrorism around the world.

The plaintiffs, family members of victims of attacks in Israel, argue that three foreign banks with U.S. branches should have known to block transactions involving certain charities because they were on other countries' terror watch lists.

The banks — Arab Bank of Jordan, Royal Bank of Scotland Group PLC's National Westminster Bank PLC, and Credit Agricole SA's Credit Lyonnais of France — say that they followed all relevant U.S. laws and that, in the vast majority of the events cited in the lawsuits, the Treasury Department had not yet identified the alleged perpetrators as terrorists.

Experts said rulings against the banks could have a broad impact on the anti-laundering system.

"If the plaintiffs are successful, ... the practical effect will be to raise the bar to a different and much higher standard of whether the bank reasonably could have formed a suspicion, based on a search for publicly available information, that their customers were involved in financing of terrorism or other terrorist activities," said Ross Delston, an anti-laundering consultant and the founder of GlobalAML.com.

"This would be a change of volcanic proportions, literally changing the landscape for banks in their relationships with their customers, since no law, regulation, or international standard that I am aware of requires this to be done in order to combat the financing of terrorism," he said.

The Financial Crimes Enforcement Network fined Arab Bank $24 million in 2005 for problems with its anti-laundering program, including lax controls — a fine the bank said was unjustified. However, the new suits go further. They allege that the bank knowingly provided services to a charity linked to terror.

Previous cases of this kind have been thrown out of court, and experts said that they believe the New York suits are the first of their kind to move forward, and that they could spur additional ones.

"It's a very new concept saying that the failure of a bank to comply with AML would make them liable for domestic or international crime," said Peter Djinis, an anti-laundering consultant and a former Federal Crimes Enforcement Network official. "No question it could open the door to more cases."

To date, 13 suits are pending in New York, with the earliest filed in August 2004 and the most recent last month.

The plaintiffs in all the cases — two against Credit Lyonnais, two against National Westminster, and nine against Arab Bank — allege that the banks knowingly provided financial services to charities with links to terrorist organizations and are therefore partly to blame for attacks from 2000 through 2003 in Israel.

They cite designations by other countries, including Israel, as proof the banks should have known the charities had terrorist ties, since information that cast suspicion on the charities' activities was publicly available.

Michael Elsner, a lawyer at Motley Rice LLC representing plaintiffs who are suing Arab Bank, argued that the bank must be held accountable. "Banks are almost always used in financing terrorism, and if the victim of a terrorist act can't hold a bank accountable, the enforcement of terrorism does not have any teeth."

Stephen Kroll, a former Democratic special counsel for the Senate Banking Committee and a former Fincen official, said the cases against Arab Bank are the most significant, because they involve people who are not U.S. citizens and are being tried under the 1789 Alien Tort Claims Act. The law grants foreigners the right to sue in U.S. courts for crimes "in violation of the law of nations," such as genocide, even for acts committed outside the United States.

The Arab Bank cases are the only suits involving foreign plaintiffs. "These decisions really do broaden out the definition," Mr. Kroll said. "It means any bank in the world with an office in the U.S. could be liable if found aiding and abetting terrorism. Given the size of some banks with international clients, it could have broad implications."

The banks say they followed proper anti-laundering procedures. Robert Chlopak, a partner at Chlopak, Leonard, Schechter and Associates, a public relations firm that represents Arab Bank, said it "condemns terrorism of any kind, and the bank has not and would not do business with any person or organization" known to be involved in terrorism.

"The plaintiff's legal theories in the cases already filed against three banks pose a potential risk to the industry," Mr. Chlopak said. "If successful, they could expose global banks to unprecedented legal and financial liability in the United States for transactions executed outside this country in full compliance with applicable national banking laws."

Credit Lyonnais said that it had no way of knowing the charities were connected with terrorism, and that all financial activities with accused charities occurred before they were designated as such by U.S. authorities.

Linda Harper, a Royal Bank of Scotland spokeswoman, said National Westminster had "no knowledge of the alleged terrorist activities" of the charities named in the complaint and disagreed with a September court decision allowing the case to go forward.

The bank "strongly believes that the legal claims against NatWest are unfounded," Ms. Harper said. "NatWest remains confident that its defense of the U.S. proceedings will prevail."

Anti-laundering experts acknowledge that banks must go beyond simply checking for U.S. designations when investigating a customer's activities. But they also question whether a bank should be held criminally responsible if a customer uses an account to fund terrorism.

Terrorist financing often lacks the hallmarks of traditional money laundering and involves very small-dollar wire transfers, the experts said.

"Given the fact that most terrorists have no criminal record, are dealing in small financial transactions, and are engaged in innocuous activities, having the banks do this kind of enhanced due diligence will not be very effective," Mr. Delston said.

Chris Myers, a partner at Holland & Knight LLP and a co-chairman of its global compliance and governance practice, said these cases are using anti-laundering standards as public liability standards.

"You can't expect us to be out in front of the federal government," Mr. Myers said. "We cannot be and are not equipped to be the police."

David Caruso, the chief executive officer and managing director of Dominion Advisory Group LLC, a Centreville, Va., anti-laundering consulting firm, said the potential implications of these cases are severe, because they would put the burden of finding a crime on the bank.

"These types of suits may have merit only if prosecutors ... are able to prove these banks failed to identify criminal acts and that failure was criminal," he said.

granting options to purchase M&T stock can give employees, as I wrote in a letter on this topic in August 2004, "...a stake in the success of our bank. Ultimately this yields a dedicated team of employees working to make M&T the best bank."

It's important to note that our option grants are not limited to a small coterie of upper management. Within the last ten years, 9,138 active employees (other than Management Group members) have been awarded a total of 11.9 million stock options. Of those employees, 2,540 hold 4.8 million of vested, but as of yet, unexercised options with an intrinsic value of approximately $228 million. Our records show that, on average, M&T employees who have been awarded stock options have waited about 6.5 years before exercising those options, despite having become vested years earlier. They have, in other words, chosen to retain a stake in the long-term growth prospects of M&T rather than to realize a short-term gain.

The larger point here is this. We well understand we face serious competition for capable employees at all levels—and are not leaving the hiring of new talent to chance. Rather, we have organized a series of focused efforts which have been consistently successful and which have and will serve as the means to rejuvenate and reinvigorate our workforce, as we have grown and will grow further.

THOUGHTS ON REGULATION AND COMPLIANCE

We have noted on a number of occasions in this space in previous years that the cost of regulatory compliance has become significant. In a period in which the challenge of continuing growth in net income has itself become greater, the significance of regulatory compliance cost has become even more notable. Businesses of all kinds are subject to a great many forms of regulation and properly so—although, as we noted in this space last year, we join many others in questioning whether some sections of the Sarbanes-Oxley Act lead to benefits commensurate with their costs; we have been particularly concerned about the section requiring reporting on internal control systems which we estimate, in the year past, cost M&T an additional $2 million with which to comply—and yet was mainly a formalization of costly reporting of checks that any well-run firm would want to have. Part of this expense included training approximately 150 employees within the organization of their role in implementing these new reporting requirements.

There has been a good deal of public and official attention paid to the issue of whether sections of the Sarbanes-Oxley legislation have led to benefits commensurate with their costs. There has, however, been surprisingly little attention addressed to other recent legislation whose regulatory requirements have proven far more significant for banks, including M&T. I refer here to Bank Secrecy Act, Anti-Money Laundering Acts, and USA PATRIOT Act requirements (collectively "AML Regulations"). The annual recurring direct expense of compliance with AML Regulations for M&T Bank is approximately $3.3 million—almost twice that being spent on Sarbanes-Oxley compliance. This expense is primarily comprised

of human resource expenses related to 47 employees dedicated to researching and filing with the government reports of currency transactions and reports of activity deemed to be "suspicious" of violating AML Regulations plus annual technology expenses to maintain the systems those employees use. Prior to the events of September 11, 2001, the annual costs were approximately $300,000 for 6 employees. In addition to the significant growth in these annual recurring expenses, over the past two years, M&T Bank incurred approximately $8.8 million in non-recurring costs for structural enhancements to its programs including new technology systems—with an additional $800,000 anticipated for 2007. Training related to AML Regulations is also expensive. Each and every employee receives basic training annually. In addition approximately 3,500 branch personnel require enhanced training on the so-called "know your customer" requirements of the AML Regulations. The point here is both that these costs are of a significant magnitude and that, although costs associated with AML Regulation compliance are far greater than costs associated with Sarbanes-Oxley compliance, the latter is, albeit belatedly, being publicly scrutinized through a cost-benefit analysis (particularly in the work of the Public Company Accounting Oversight Board), the former is not. Indeed, it can be said that virtually everyone at M&T who deals directly with customers is made increasingly less productive because of regulatory compliance.

AML Regulations fall within a relatively new category of regulation focused on protecting the public at large and the reputations of banks from illegal behavior engaged in by bank customers. Recognizing the clearinghouse role that they play in the economy, banks are increasingly being required by such regulations to identify, retain and report information that may potentially be useful in criminal investigations. Of course, notwithstanding that degree of difficulty, there is a rationale behind such regulation. Mandates associated with the Bank Secrecy Act, Anti-Money Laundering Acts and other legislation that aid law enforcement are predicated on the principle that tracking—and potentially blocking—financial transactions of a suspicious nature can both reveal the identity of those involved in terror plots and other criminal activity and, it is hoped, starve such enterprises of funds. It is a sensitive matter to suggest, as we did here last year, that the cost of such effort might not be close to commensurate with public benefits realized—or that this regulatory regime amounts to a sort of unfunded mandate which the shareholders of M&T and other financial institutions are asked to bear for the public at large. It is, however, at the very least worth looking at the cost details of regulatory compliance in these areas so as to have an informed discussion about such matters.

Compliance with the Bank Secrecy and Anti-Money Laundering Acts can be thought of as an elaborate filtering process to which numerous M&T employees are dedicated. They must scan each and every financial transaction which we facilitate and then devote special attention to a growing minority of transactions, chosen from amongst all others based on rules such as the amount of cash involved or whether they take place via wire transfer of funds.

Vast numbers of customer transactions are scrutinized. A much smaller number lead us to filing currency transaction reports or so-called Suspicious Activity Reports ("SARs");

a much smaller number still lead to any sort of follow-up with us by the authorities. The extent of this work was great in 2006. Our employees investigated over 406,500 currency transactions to determine whether follow-up reporting was necessary and ultimately filed 141,736 currency transaction reports. In addition to monitoring deposits and withdrawals of currency, 4,970 instances were investigated to determine whether those customer transactions were suspected of violating AML Regulations. These investigations resulted in the filing of 886 SARs. Employees spent some 70,000 hours investigating transactions suspected of violating AML Regulations and, in the process, determined that the overwhelming majority of this activity was utterly benign, a mere reflection of normal business activity such as that in which small retail businesses routinely engage. For the second consecutive year, only 10 of those investigations led to significant follow-up inquiry to us from authorities.

The story was similar as relates to wire transactions which we are required to monitor by the United States Department of Treasury's Office of Foreign Assets Control, or OFAC. That office is responsible for enforcing economic sanctions against nations or specific individuals targeted for such reasons as the possible role in narcotics trafficking or terrorism. All industries must seek to comply with such sanctions—but the banking industry is particularly affected; it is required to block funds that may be passing through a bank (including via wire transfer) and meant to finance illicit activity. Banks must establish procedures to scan all such transactions to ensure that they are not subject to OFAC rules. Like the monitoring of deposits and withdrawals, this transfer tracking process is a major undertaking. In 2006, M&T Bank processed nearly 1.6 million wire transactions—each one had to be electronically scanned to make sure it did not match a nation or individual on an OFAC list. Although 48,000 were judged to be in need of further review, we were ultimately required to block only a single transaction—for $530.00.

Yet more such reporting requirements are on the way. A new (2006) law concerning the payment of illegal Internet gambling debts will likely add additional burdens on the financial services industry to attempt to identify, investigate and report such transactions. We are awaiting regulations to implement this law that are due to be issued in July of 2007. Depending on how the regulation is ultimately crafted, this law may well impose upon financial institutions a burden that would be analogous to finding a needle in a haystack located on a moving truck.

It is true, of course, that it could be crucial to the security of the United States to block even one questionable transfer of funds—if that transfer were to make possible a terrorist act. Yet it is worth asking whether it is sensible to monitor such a large number of transactions, of which those monitored by M&T are but a small fraction of those reviewed by all banks, nationwide. Might it make more sense, for instance—as judged by the resources invested in the process—for banks to be required to provide such records on demand, on those occasions when police surveillance or arrests lead law enforcement officials to believe that financial transactions can provide crucial evidence? Might it even be the case that the

resources of law enforcement are being diluted by virtue of having to review so many reports from banks across the country? We would hope that, as a general rule, government would approach AML Regulation on a cost-benefit basis, with an eye toward an effort—on the part of both public officials and private industry—which goes beyond busywork and is, rather, effective in keeping American citizens safe.

It is worth noting that in addition to the new requirements of Sarbanes-Oxley and bank secrecy and anti-money laundering-related rules, banks continue to comply with a wide range of regulations from the Federal Reserve, state banking departments and others in keeping with government's historic interest in financial institutions protecting depositors through sound management of credit, liquidity and interest rate risks—so-called "safety and soundness regulations." These have been augmented in recent years by regulations focused on protecting bank consumers from inappropriate practices, such as unlawful discrimination and unfair or deceptive acts and practices. These types of regulations, long a part of banking, have continued to increase in cost and complexity even as the other new and demanding regulations described above have taken effect.

Of course, compliance with regulations cannot be easily ascribed to any particular number of employees. Compliance is pervasive and part of every employee's day-to-day duties. The increased compliance responsibilities that become woven into the fabric of every employee's workday are immeasurable but nonetheless real. For example, there are real costs associated with a customer service representative spending time to ask customers for additional information required by regulations or the effort expended by Finance Division employees to prepare additional reports required by regulations. Every time regulatory burdens are increased, there are immeasurable costs associated with identifying those employees impacted, training those employees and the additional time those employees take to perform their normal daily functions thereafter. These additional costs are real, are likely very large but are nearly impossible to capture and thus seem to largely be ignored by policymakers.

It's our hope that by focusing attention on such regulatory costs, we will ultimately minimize regulatory burdens while maximizing the benefits to those whom the regulations seek to protect.

UPSTATE NEW YORK

I have frequently expressed, both in this space and in a variety of public forums, my profound concern about the condition of the economy of the upstate New York region in which M&T is headquartered. Limited job growth and an ongoing outmigration of young people (recently confirmed by the Census Bureau, which found that New York State lost more of its population in 2006 than any state other than post-Katrina Louisiana) are both causes and symptoms of this lackluster condition. It is, then, with a sense of hope and satisfaction that I note that new political leadership in New York State has signaled its intention to make revival of Upstate one of its top priorities.

Testimony of Salvador Hernandez
Deputy Assistant Director
Criminal Investigative Division
National Crimes Branch
Federal Bureau of Investigation
Before the Committee on Financial Services
Subcommittee on Oversight and Investigations
May 10, 2007

Introduction

Good morning Mr. Chairman, Ranking Member Miller and members of the subcommittee. On behalf of the Federal Bureau of Investigation, I am honored to appear before you today to discuss how the FBI successfully utilizes information obtained from the private financial sector. Chief among the investigative responsibilities of the FBI is the mission to proactively neutralize threats to the economic and national security of the United States of America. Whether motivated by criminal greed or a radical ideology, the activity underlying both criminal and counterterrorism investigations is best prevented by access to financial information by law enforcement and the intelligence community. The FBI considers this information to be of great value in carrying out its mission to protect the citizens of this country, and over the past few years, we have made significant advances in utilizing this information to carry out our mission.

In the "criminal greed" model, the FBI utilizes a two-step approach to deprive the criminal of the proceeds of his crime. The first step involves aggressively investigating the underlying criminal activity, which establishes the specified unlawful activity requirement of the federal money laundering statutes, and the second step involves following the money to identify the financial infrastructures used to launder proceeds of criminal activity. In the counterterrorism model, the keystone of the FBI's strategy against terrorism is countering the manner in which terror networks recruit, train,

plan and effect operations, each of which requires a measure of financial support. The FBI established the Terrorist Financing Operations Section (TFOS) of the Counterterrorism Division on the premise that the required financial support of terrorism inherently includes the generation, movement and expenditure of resources, which are oftentimes identifiable and traceable through records created and maintained by financial institutions.

The analysis of financial records generated by the private financial services sector provides law enforcement and the intelligence community real opportunities to proactively identify criminal enterprises and terrorist networks and disrupt their nefarious designs.

Traditional Criminal Money Laundering Investigations

Money laundering has a significant impact on the global economy and can contribute to political and social instability, especially in developing countries or those historically associated with the drug trade. The International Monetary Fund estimates that money laundering could account for two to five percent of the world's gross domestic product. In some countries, people eschew formal banking systems in favor of Informal Value Transfer systems such as hawalas or trade-based money laundering schemes such as the Colombian Black Market Peso Exchange, which the Drug Enforcement Administration estimates is responsible for transferring $5 billion in drug proceeds per year from the United States to Colombia. Hawalas are centuries-old remittance systems located primarily in ethnic communities and based on trust. In countries where modern financial services are unavailable or unreliable, hawalas fill the void for immigrants wanting to remit money home to family members, and unfortunately, for the criminal element to launder the proceeds of illegal activity.

There are several more formalized venues that criminals use to launder the proceeds of their crimes, the most common of which is the United States banking system, followed by cash intensive businesses like gas stations and convenience stores, offshore banking, shell companies, bulk cash smuggling operations, and casinos. Money services businesses such as money transmitters and issuers of money orders or stored value cards serve an important and useful role in our society, but are also particularly vulnerable to money laundering activities. A recent review of Suspicious Activity Reports filed with the Financial Crimes Enforcement Network

(FinCEN) indicated that a significant number of money services business filings involved money laundering or structuring.

The transfer of funds to foreign bank accounts continues to present a major problem for law enforcement. Statistical analysis indicates that the most common destinations for international fund transfers are Mexico, Switzerland, and Colombia. As electronic banking becomes more common, traditional fraud detection measures become less effective, as customers open accounts, transfer funds, and layer their transactions via the Internet or telephone with little regulatory oversight. The farther removed an individual or business entity is from a traditional bank, the more difficult it is to verify the customer's identity. With the relatively new problem of "nesting" through correspondent bank accounts, a whole array of unknown individuals suddenly have access to the U.S. banking system through a single correspondent account. Nesting occurs when a foreign bank uses the U.S. correspondent account of another foreign bank to accommodate its customers. A foreign bank can conduct dollar-denominated transactions and move funds into and out of the United States by simply paying a wire processing fee to a U.S. bank. This eliminates the need for the foreign bank to maintain a branch in the United States. For example, a foreign bank could open a correspondent account at a U.S. bank and then invite other foreign banks to use that correspondent account. This would then cause the U.S. bank to not know the actual individual or entity conducting the transaction.

The FBI's pending money laundering cases include examples of proceeds generated from criminal activities such as organized crime, drug trafficking, fraud against the government, securities fraud, health care fraud, mortgage fraud, and domestic and international terrorism. By taking a two-step approach to these investigations; step one being the investigation of the underlying criminal activity and the second step being following the money, the FBI has made significant inroads into identifying the financial infrastructure of the domestic and international criminal or terrorist organizations. Once the underlying criminal activity is identified and the financial infrastructure has been discovered the FBI has aggressively applied the asset forfeiture laws in order to seize and forfeit the proceeds of the illegal activity.

In recent years the international community has become more aware of the economic and political dangers of money laundering and has formed alliances on several fronts to share information and conduct joint investigations. Members of the Egmont Group, a consortium of Financial

Intelligence Units (FIU) of which the United States is a member, can access a secure website developed by FinCEN (the United States' FIU) to share vital information on money laundering between participating countries. In a further demonstration of international cooperation, the international community [over 150 nations] has endorsed the 40 anti-money laundering recommendations and the nine anti-terrorist financing recommendations of the Financial Action Task Force (FATF). As it relates to international money laundering enforcement, the FBI is an active participant in the United States' delegation to the FATF. Since its creation, the FATF has spearheaded the effort to adopt and implement measures designed to counter the use of the financial system by criminals. It issued a slate of 40 recommendations in 1990, which were revised in 1996 and again in 2003, to ensure that the approach they create remains current and relevant to the evolving threat of money laundering. The FATF's 40 recommendations on money laundering and nine recommendations on terrorist financing together set out the framework for anti-money laundering and counter terrorist financing efforts and are of universal application. All member countries have their implementation of the forty recommendations monitored through a two-pronged approach: an annual self-assessment exercise and a more detailed quadrennial mutual evaluation process. The FBI participated in the recent FATF mutual evaluation of the United States' compliance with the 40 anti-money laundering and the nine counterterrorist financing recommendations.

Terrorism Investigations

Access to financial information significantly enhances the ability of law enforcement and members of the intelligence community to thwart terrorist activity. The lack of complete transparency in the financial regulatory system is a weakness on which money launderers and financiers of terrorism rely to reap the proceeds of their crimes and to finance terrorist attacks. Limited access to financial records inhibits law enforcement's ability to identify the financial activities of terror networks. Efforts to detect terrorist activity through financial analysis are further complicated by the fact that the funding of terrorism may differ from traditional money laundering because funds used to support terrorism are sometimes legitimately acquired, *e.g.*, charitable contributions and the proceeds of legitimate business. Overcoming these challenges so we can prevent acts of terror has increased the importance of cooperation with our partner law enforcement agencies, the intelligence community, and the private financial and charitable sectors.

Records created and maintained by financial institutions pursuant to the Bank Secrecy Act (BSA) are of considerable value to these critical efforts. The FBI enjoys a cooperative and productive relationship with FinCEN, the purveyor of BSA information. FBI cooperation with FinCEN has broadened our access to BSA information which, in turn, has allowed us to analyze this data in ways not previously possible. When BSA data is combined with the sum of information collected by the law enforcement and the intelligence communities, investigators are better able to "connect the dots" and, thus, are better able to identify the means employed to transfer currency or move value.

The result of this collaborative relationship and access to financial intelligence is a significant improvement in the efficiency of our investigation of terrorist financing matters.

The ability to quickly and securely access and compare BSA data to classified intelligence and law enforcement information is critical. Sometimes the investigative significance of a BSA filing cannot be appreciated until the items included on the document are compared against predicated law enforcement or intelligence information that may not be of the public record. Such critical information can be biographical or descriptive information, the identification of previously unknown associates and co-conspirators, and, in certain instances, the location of a subject in time and place. In addition the BSA filings can also include the identification of other bank accounts, assets or banking relationships that were previously unknown to the investigation. Abundant anecdotal examples exist of activities noted in BSA reports which have added value to counterterrorism and criminal investigations, oftentimes in ways that could not have been predicted from the reports alone. BSA data allows for a more complete identification of the respective subjects such as personal information, non-terrorism related criminal activity, bank accounts, previously unknown businesses and personal associations, travel patterns, communication methods, resource procurement, and Internet service providers.

The value of BSA data to our anti-money laundering and counterterrorism efforts cannot be overstated; the importance of access to that information has already proven invaluable on the micro, or individual case level, as well as on the macro, or strategic level. BSA data has proven

its great utility in counterterrorism matters, and any contemplated change to the underlying reporting and recordkeeping requirements of the BSA should be measured and carefully considered before such action is taken.

While the Suspicious Activity Report (SAR) is also an extremely valuable tool and has provided significant operational uplift, the suggestion that a SAR requirement could effectively substitute for the intelligence gleaned from a CTR misunderstands the differences between the requirements and the manner in which they complement each other. CTRs are objective reports that document an event in time, providing such information as the identity of the transactor, the bank name, account number, account owner, and dollar amount. Additionally, these reports are available for at least a ten-year period, and investigators and analysts have the ability to directly query these reports when necessary.

In contrast, SARs are available on select matters where a bank official has made the subjective determination that a particular transaction or activity is suspicious. Although the banks are doing an outstanding job on reporting suspicious activity, SARs are not a substitute for the objective transaction reporting provided by CTRs. Additionally, since banks are not privy and do not have access to the same information as law enforcement or the intelligence community, many CTRs may be filed before a bank may be able to identify and report the activity as suspicious, provided they are even able to reach that determination from the information available to them. Also, the 314(a) process, designed to promote cooperation among financial institutions, regulatory authorities, and law enforcement authorities, can only be used on the most significant terrorism and money laundering investigations, and only after all other financial leads have been exhausted, which include reviewing CTRs. The financial institutions are only required to review accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months, in sharp contrast to the ten years of data provided by the CTRs. Moreover, all three tools, complementary and collectively, are of tremendous value.

Use of CTR and BSA Data

In respect to the FBI, the FBI has direct access to FinCEN's BSA database and we receive regular updates of BSA reports for ingestion into the FBI's Investigative Data Warehouse. The FBI works closely with it law enforcement counterparts in the utilization of SARs, for example the FBI participates in Suspicious Activity Report Review Teams around the country. These methods allow us to conduct robust analysis on a pro-active and re-

active basis. In addition, the FBI works closely with FinCEN. The FBI has a Supervisory Special Agent from the Financial Crimes Section serving as a Liaison between the FBI and FinCEN. Assisting this liaison are FBI analysts and other professional support personnel

SAR/CTR and BSA data is used in a myriad of ways. Whether or not SAR/CTRs drive an investigation or are confirmatory, is wholly dependent upon the type and nature of the investigation. They can and have been the impetus for an investigation in addition they can add significant value to ongoing investigations by providing previously unknown subjects/co-conspirators, accounts and banking relationships to name just a few. The FBI has taken pro-active steps to further examine this information. Utilizing technology we are able to identify financial patterns associated with money laundering, bank fraud, check fraud, and other aberrant financial activities. However, while SARs have been regarded as traditional indicators of criminal activity, these records may reveal evidence of terrorism and intelligence activities as well. The identification of criminal financial links will provide leads for criminal investigations. Leads developed from analysis of SAR activity may be instrumental in "connecting the dots" for cross-program investigations of criminal, terrorist and intelligence networks, all of which rely on financial transactions to operate. Application of technology enables agents and analysts to visualize financial patterns, link discrete criminal activities, and display the activities in easily readable formats for use in cases.

The FBI works closely with our State and Local partners in task force environments, to include our Joint Terrorism Task Forces and others that are established at either the Field Office or national level. In addition, State and Local law enforcement have access to BSA data through state coordinators designated by FinCEN.

If there is any doubt that law enforcement vigorously and proactively utilizes BSA data, and especially SARs, I would like to dispel that doubt right now. Federal law enforcement agencies review and utilize SARs in a proactive manner to identify both potential money laundering cases as well as money laundering trends. Moreover, as indicated in the 2007 National Money Laundering Strategy that was released last week, law enforcement agencies do not review the SARs in isolation. The Departments of Justice, Treasury, and Homeland Security encourage the formation of interagency SAR review teams to review and discuss the SARs in a coordinated manner, in order to exchange information and avoid duplication of effort. There are

80 SAR Review Teams operating across the United States analyzing BSA data to identify evidence of financial crimes and money laundering. In many cases, these groups include representatives from state and local law enforcement. The investigations resulting from these task forces frequently result in successful investigations of money laundering, fraud, drug trafficking, and other offenses. While we are limited in our ability to discuss such cases openly because of the confidentiality requirements surrounding SARs, we would welcome the opportunity to provide you with examples of such successful investigations.

In conclusion, BSA data is invaluable to both our counterterrorism efforts and our more traditional criminal investigations. Our experience shows that terrorism activities are relatively inexpensive to carry out and that the utilization of data obtained pursuant to the BSA provides significant operational uplift. The FBI is committed to collaborating with this Committee and the Congress to ascertain whether certain categories of the BSA can be reworked without harm to our investigative capabilities. The GAO is currently studying this issue, with a report due in early 2008, and the FBI has been an active participant in this study. However, to alter the current BSA reporting requirements -- without careful study to determine the range of implications -- could be a significant setback to investigative and intelligence efforts relative to both the global war on terrorism and traditional criminal activities.

Testimony of

Megan Davis Hodge

On Behalf of the

American Bankers Association

Before the

Subcommittee on Oversight and Investigations

Committee on Financial Services

United States House of Representatives

May 10, 2007

Testimony of

Megan Davis Hodge

On Behalf of the

American Bankers Association

Before the

Subcommittee on Oversight and Investigations

Committee on Financial Services

United States House of Representatives

May 10, 2007

Chairman Watt and Members of the subcommittee, I am Megan Davis Hodge, Director of Anti-Money Laundering and BSA Officer for RBC Centura Bank, headquartered in Raleigh, North Carolina appearing today on behalf of the American Bankers Association (ABA). ABA, on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership – which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks – makes ABA the largest banking trade association in the country.

ABA and its members have long been steadfast partners with law enforcement and regulators in the mission to protect the integrity of the American banking system against the threat of serious illegal financial activity, money laundering and terrorism financing. From the Board room through senior executives and compliance professionals to tellers and other transaction personnel, the banking industry strives to deter, detect and defend against those who would undermine our financial system.

While vigilance is high to combat threats against our financial and economic system, the issue before us today is how to use the resources available to all parties in the most effective way to increase our success.

This hearing, Mr. Chairman, is extremely timely and important. ABA appreciates this opportunity to address how banks, regulators and law enforcement can improve the Suspicious Activity Report (SAR) process and make Bank Secrecy Act (BSA) compliance requirements more responsive to the challenges we all face in combating money laundering, terrorism financing and serious financial crime. This mission is too important to squander our resources on ineffective reporting programs. We need to give priority to the efforts that achieve the greatest benefit and eliminate those obligations that produce relatively little or no benefit.

The general themes of my testimony are:

- Standards for suspicious activity reporting should be fine-tuned to assure it encourages and enables effective reporting and better balances burden with benefit.

- Antiquated reporting obligations should be eliminated as they have a low degree of usefulness in combating financial crime and divert resources away from newer, more effective methods.

- Finding cost-effective solutions to minimize the direct and opportunity costs of BSA data reporting is critical. The cost is significant and rising for all banks. For small community banks, resource challenges in implementing new software, dedicating staff to review outputs, and managing the documentation and reporting requirements of anti-money laundering programs are becoming severe.

Under these themes, we recommend the following:

- Uniform Examination Procedures provide a solid foundation for consistent supervision, but refinements are needed, such as allowing SARs to be shared within an enterprise-wide BSA compliance program.

- Through training and consistent application, assure that examiners abide by the Interagency Exam Procedures, which will reduce banks' very real concerns about being second-guessed by the examiners and reduce marginal or "defensive" SAR filings.

- Better communicate law enforcement priorities, results and limits, through more realistic threshold requirements for SAR filing that conform with law enforcement prosecutorial standards; distribution of SARs to specialized teams that can detect patterns and more effectively pursue such crimes as identity theft and mortgage fraud; establishment of a rule that stops filing after the second SAR if law enforcement has not indicated a specific interest in that customer's continuing activity; and instituting tracking by the Financial Crime Enforcement Network (FinCEN) and the Justice Department of outcomes associated with the use of SARs.

- Update the archaic currency transaction report (CTR) system by eliminating CTRs on seasoned customers, which would, in turn, make the SAR process much more effective and efficient.

- Reconsider the IRS approach to investigating structuring SARs and develop a communication strategy to better educate bank customers about BSA data reporting in order to discourage idiosyncratic structuring behavior without jeopardizing the confidentiality in SAR filings.

The remainder of my statement will detail these themes and recommendations.

Uniform Examination Procedures are a Solid Foundation for Consistent Supervision

At ABA's prior appearance before this subcommittee in May 2005, we emphasized that the banking agencies needed to reach agreement on how the financial services industry would be examined for compliance under the USA PATRIOT Act and the other anti-money laundering (AML) requirements. Under the auspices of the congressionally authorized Bank Secrecy Act Advisory Group (BSAAG), bank representatives were able to provide suggestions to agency staff during their drafting process. Bankers were seeking useful guidance for developing compliance programs that would meet supervisory expectations and also respect management's risk-based judgments about tailoring controls to each bank's unique operations. We believe the willingness of the agencies to engage with the private sector resulted in procedures that better anticipated the needs of bankers.

We are pleased to note that the final interagency procedures were released on June 30, 2005. FinCEN, the federal banking agencies and ABA (together with other bank trade associations), coordinated extensive outreach efforts to both examiners and bankers to introduce the Interagency Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual to the industry.

However, there are still areas where our bankers have suggested improvements in the procedures. One important disconnect between the goal of effective reporting and the manual's guidance is in the area of sharing SARs among sister affiliates within an enterprise-wide BSA compliance program. On the one hand, the manual states that "banking organizations should not share SARs with such affiliates." Yet on the other hand, enterprise-wide risk management is encouraged by the Interagency Exam Procedures – and the most natural option to effectuate such a program includes the freedom to share SARs across sister affiliates within the organization in a secure manner. Although the BSAAG Subcommittee on SARs and the ABA have recommended guidance that approves such sharing, FinCEN and the agencies have not yet updated their policy statements despite pledging over a year ago to do so. Thus, today, we continue to labor under the counterproductive constraint in the manual that banking organizations should not share SARs with sister affiliates. Such sharing not only allows banks to take their own prudent actions against suspicious activity across the enterprise, but it also increases the likelihood of better and more complete information – within a fuller context – to be shared with law enforcement services.

Of course, as with any new procedures, implementation is the real test of their success. At this time, ABA sees the glass half-full in that regard. In particular, how the exam procedures are applied to bank SAR processes and how agencies administer SAR utilization are issues that will have significant impact on the burden banks bear, and the benefit government derives, from suspicious activity reporting going forward.

The SAR Process is Burdensome and Leads to Unwarranted Reporting

In the words of the Interagency Exam Procedures, "suspicious activity reporting forms the cornerstone of the BSA reporting system." Perhaps reflecting its place as the cornerstone of BSA compliance, the section of the Interagency Exam Procedures on SARs is 17 pages—the longest section in the more than 300-page manual. Yet even this is an underestimation; most of the rest of the manual is guidance on how to detect and mitigate a range of potential financial crime risks

across the spectrum of bank operations and products, demonstrating that the entire volume sets forth expectations that engage every corner of the bank in the task of reporting suspicious activity.

No matter what their size, banks have an ongoing obligation to monitor their customers' transactions and banking behavior in order to detect suspicious activity. To undertake this duty, an institution must start by assessing and understanding the money laundering and terrorist financing risk of its customers and the products they use in order to build a transactional profile that facilitates identification of anomalies and unusual patterns. Detection may be triggered by the personal observation of a teller or other customer service personnel—or it may occur as a result of a manual or automated back-office review of transaction records. Once a transaction, or series of transactions, is flagged for unusual behavior, an investigation is conducted into the details of the suspect behavior. After this detailed review, a SAR is filed if the bank has reason to believe that the customer's activity meets the reporting requirements. Compliance with filing deadlines, transaction threshold levels and report narrative requirements are observed throughout the process. Extensive records are generated and maintained as part of the process to support the SAR or even the decision ***not*** to file a SAR.

Informing senior management about the bank's SAR experience takes place on an ongoing basis and the independent audit function ensures that the overall SAR process is sound and completed in a timely manner. As with other AML/BSA obligations, employee training, risk-reassessment, documentation and retention are layered on top of the linear monitoring and filing process.

Yet this brief summary does not do justice to explaining what it really takes to comply with SAR procedures, nor does it fully convey the expense and opportunity cost incurred in the process. Even those adopting automated technology solutions face both information technology costs and considerable manual investigatory effort. Although systems are put in place for account and customer monitoring, they require manual intervention to investigate each alert that is produced on a daily basis, which can amount to hundreds if not thousands of transactions flagged. Additionally, institutions must document the automated monitoring process from end to end, from developing the daily data feed that goes into the specialized detection software to training staff on how to handle the output. Resource allocations do not stop once these systems are implemented. In addition to continued training, institutions must monitor the alert outputs and continuously adjust their filters and scenarios to reflect current or new patterns of activity, new services and products, changes in their customer base, and evolution in typical customer transactions. A clearly documented process must be followed to justify each and every change made in the system, including a rationale detailing the change to enable examiners to understand how and why modifications in monitoring levels were made. That is to say, in addition to monitoring financial activities, banks have to report on their monitoring of their monitoring.

In light of the implementation of "intelligent" software solutions, financial institutions have also had to cope with the ever rising expectations set by their examiners. As software vendors compete for the market and enhance their tools to have unique analytic capabilities, examiners are taking note of this development and doing a comparative analysis of the potential monitoring standards institutions can utilize as opposed to the basic regulatory requirements. This cycle generates escalating demands on small community banks that face resource challenges in implementing new software, dedicating staff to review outputs and managing the documentation and reporting requirements. In addition, large banks have learned from experience that while electronic monitoring solutions have utility, they have limits and do not warrant adoption just because they exist.

What has this complex and expensive undertaking produced? In the first decade since suspicious activity reporting obligations were expanded following the Annunzio-Wylie Anti-money Laundering Act, the number of SARs filed by depository institutions has grown from 81,197 in 1997 to 567,080 in 2006, a ***seven-fold increase***. As these numbers continue to rise, the question looms ever larger: Are they a measure of success or excess? Can this possibly reflect an epidemic of illicit activity eating away at the integrity of American banking? We think not. Rather, we believe that this state of reporting overdrive can be largely attributed to the following factors:

- First, regulatory pressures promote "defensive filing" that inflates SAR volume out of proportion to the risk represented by the underlying conduct.

- Second, in the absence of constructive feedback from law enforcement, banks identify a broad and evolving array of fraud and other potentially serious criminal activities that expand the SAR universe independent of the likelihood of prosecutorial pursuit or value.

Let me explore with you what might explain these points and what can be done to improve SAR process efficiencies.

Agencies Can Reduce Defensive SARs by Assuring Examiners Follow Exam Standards

During ABA's testimony in May 2005, we expressed substantial concern that regulatory scrutiny of SAR filings and the civil penalties assessed against banks for SAR deficiencies had caused many institutions to file SARs as a purely defensive tactic (the "when in doubt, file" syndrome) to stave off unwarranted criticism or second-guessing of an institution's suspicious activity determinations. If a SAR is filed, the bank cannot be criticized for not filing. This is a significant problem because defensive filing overloads the system with marginal reports and wastes bank staff time in filing technically correct, but substantively useless, information. It also wastes law enforcement time and resources in processing and evaluating these surplus SARs. In a world of SARs, more is not better; unfortunately, the current system succeeds only in extracting more.

Every ABA member bank wants to eliminate defensive filings and have the satisfaction of knowing that its anti-money laundering efforts are making a difference in thwarting crime and terrorism. However, ABA members continue to comment that unwarranted substitution of examiner judgment for their own bank's well-considered risk assessment is the reason for these defensive filings. We believe that much of the solution to this serious problem resides in eliminating fear of supervisory second-guessing by making sure examiners respect the bank's risk assessment and abide by the review standards established in the Interagency Exam Procedures. These procedures focus on effective programs, not quantitative outputs. The procedures state:

> The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the

> bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[1]

We believe this standard is sound and that the banking agencies intend to abide by it. The challenge for our regulators is to assure that examiner judgment is trained and applied in a way that supports this standard and honors the risk-based approach endorsed by the manual. ABA believes that this does not require legislation, but can be addressed through Congress's oversight powers. We support holding the agencies accountable for monitoring and correcting deficiencies in how examiners apply this standard. We believe that codifying this standard places would be unnecessary and could actually impose regulatory rigidity where risk-based flexibility is preferred. Moreover, it would not improve upon what has already been succinctly stated by the agencies themselves. As long as any criminal prosecution of SAR filing deficiencies is subject to existing Justice Department guidance involving consultation with the banking regulators, banks should feel more secure about making the judgments called for in filing quality SARs.

Another practice could be adopted by the agencies to help the industry assure better examiner analysis of the SAR process—especially when conducting reviews of individual SAR decisions. Although examiners receive bank specific reports about an institution's SAR filings in preparation for an exam, they refuse to share those reports with the subject bank at the exam. We have members who report they have spent extensive time and effort responding to examiner inquiries that in the end turned out to have been based on inaccuracies in the reports the examiner had received from his agency. We believe that if examiners shared these reports from the beginning, we could eliminate inaccuracies rather than engage in wasteful searches predicated on erroneous information. After all, the compliance exam is not supposed to be a report-by-report "gotcha." Rather, exam transaction testing is intended to evaluate overall program quality.

I would like to now turn to the second point dealing with the real law enforcement value of SARs.

Better Communicate Law Enforcement Priorities, Results and Limits

Substantial bank resources and many SAR filings apply to financial crimes that cause banks and their customers to suffer significant losses. Crimes such as fake check and wire scams, credit and debit card fraud, mortgage fraud, identity theft, and computer intrusion are being reported and contribute to a rising trend in SAR filings. Still, compliance professionals realize that not every SAR will yield an active law enforcement case or even become a corroborating lead in such a case. This is due to several factors. One significant factor is that the thresholds for filing SARs are far below the operative thresholds used to guide prosecutorial discretion. After all, law enforcement does not have unlimited resources. Banks do not have unlimited resources either, and we would rather not flood the system with filings that are not going to be acted on. ABA has several suggestions to address this:

- FinCEN should review the threshold requirements for SAR filing and recommend more realistic levels that are likely to conform to law enforcement prosecutorial standards.

[1] FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, July 2006, page 66.

- FinCEN and the Justice Department should better leverage law enforcement task forces so that SARs involving lower dollar threshold transactions are directed by type to specialized teams that can detect patterns and more effectively pursue such crimes as identity theft and mortgage fraud.

- A standard should be established that, when it comes to reporting on ***repeat*** activity, a bank can stop filing after the second SAR if law enforcement has not indicated a specific interest in the particular activity of that customer.

ABA appreciates the feedback received by the FinCEN publication, *SAR Activity Review*, and believes that it should continue. We do, however, believe that describing the value of SAR reporting must go beyond the anecdotal stories in the *Review*. In light of the enormous efforts banks expend for BSA compliance, we believe that a more probative report can be produced to enable better comparison of the burden and the benefit of the SAR process. In particular, we believe ***FinCEN and the Justice Department should institute tracking of outcomes associated with the use of SARs so that aggregated data better reflects law enforcement results*** such as cases initiated, indictments obtained, arrests, convictions and recoveries that are derived from SARs. This type of information is reported for the 314(a) process instituted under the USA PATRIOT Act and has been a great source of information to the industry.

The ABA would like to see the 314(a) data report format serve as a model for expanded reporting on outcomes of suspicious activity reporting. While the number of SAR filings and the number of indictments are not necessarily directly connected, it is interesting that between 2002 and 2005 Justice Department money laundering cases, indictments and recoveries fell while the number of SARs increased dramatically.[2] Only with more specific tracking of SAR use and case results can industry and government make more informed judgments about how to balance the burden and benefit of the SAR process and improve the focus of resources on activities that produce genuine results.

Updating the Archaic CTR System Will Go a Long Way to Improve the SAR Process

Another way of ensuring that government and industry resources are used effectively in the area of financial crime detection is to remove unnecessary data collections.

As ABA has testified on numerous prior occasions, ***we believe that the time has come to dramatically address this reporting excess by eliminating cash transaction report (CTR) filings for transactions conducted by seasoned business customers.*** ABA recognizes your strong leadership, Mr. Chairman, in pursuing such an initiative. We gratefully acknowledge your efforts along with those of your colleagues on this subcommittee and in a bi-partisan effort across the entire House that resulted in the passing of H.R. 323, the "Seasoned Customer Exemption Act of 2007" by voice vote. Enactment of this legislation could be the most significant step in years to improve the effectiveness of our anti-money laundering efforts. As any athlete knows, you improve performance when you eliminate wasted movements. Streamlining our BSA efforts will allow us to improve results.

---

[2] 2007 National Money Laundering Strategy, "FBI money laundering-related statistics, FY2002 - FY2005", Appendix B, Table F-2, Page 89.

The conspicuous consumption of bank resources for unnecessary CTRs hardly needs restating, but we note that the continued growth in CTRs last year alone prompted FinCEN to move its estimated number of filings to over 15 million per annum. Even at FinCEN's conservative estimate of around 25 minutes per report for filing and recordkeeping, it means that financial institutions as a whole devote around 6.28 million staff hours of work to handling CTRs in a single year. Based on a small sample conducted by ABA, three-quarters of bank filings were for business customers who had been with the bank for over a year. That equates to industry spending over 4.5 million staff hours filing notices on well-established, routine business customer transactions!

The two million report increase from 13 to 15 million represents the addition of more than 400 new employees throughout the banking industry dedicated to CTR reporting in one year alone! In other words, more staff were hired by industry for the increase in CTR filings than are currently employed by FinCEN. This upward trend is only likely to continue and demand more and more staff to report on more and more transactions, further burying the real needles of money laundering under an exponentially growing mound of the hay of legitimate business transactions by law abiding people recorded at great expense and ever-increasing opportunity cost.

Changing the mindset about mandating the collection of routine cash data would have the following benefits:

- The vast majority of the 15 or so million CTRs filed annually would stop, thus saving many hours a year in filling out forms;
- Wasteful SARs would decline. Rather than filing specious structuring reports, banks could focus their energies on detecting suspicious handling of currency regardless of artificial thresholds;
- Bank systems and resources could be redirected from CTR monitoring to supporting further improvement in suspicious activity reporting;
- Regulatory criticism of technical mistakes with CTR filings would cease;
- Costs incurred due to the overly complex CTR exemption process would be reduced; and,
- Law enforcement could redirect resources to better evaluation and follow-up of higher-value SARs.

Simply put, eliminating CTRs on seasoned customers is probably the single most effective step toward making the SAR process much more meaningful and efficient.

Protecting Confidentiality of SARs is Vital

Before concluding, it is important to note that for the SAR process to work properly, the safe harbor that Congress has bestowed must be vigorously defended. Only by keeping a SAR confidential and observing the prohibition against advising the subjects of a SARs that they have

been reported by the bank for suspicious activity, can we insure the safety of our bank employees and assure that the information provided will be handled securely.

Bank employees that have regular contact with customers play an indispensable role in the SAR process. This is especially true under the current system when reporting structuring behavior, i.e., when an individual seeks to conduct or structure cash transactions to be below the CTR reporting threshold. Structuring is often a matter that tellers observe in handling a customer's cash transactions. Yet recent activity by the IRS's Criminal Investigations Division (CID) has jeopardized the safe harbor protection in the process of "investigating" a structuring SAR.

ABA members in several communities around the country tell us that IRS agents and other law enforcement representatives have been literally knocking on doors at people's homes and asserting that they have information that the person is structuring their bank transactions. At the conclusion of these visits, the agent gets the individual to sign an acknowledgement so that future prosecution of the person is simplified. In other cases, letters from Supervisory Special Agents from the IRS-CID have been arriving in the mail and stating, "I have reason to believe that you, or others on your behalf, may have conducted financial transactions that appear to be in violation of the Bank Secrecy Act." Since most people do their banking at one institution, it is immediately obvious which bank has reported them to the government. In many situations, customers going through this experience confront bank employees and demand to know who reported them. Employees and managers are schooled not to confirm SAR reporting, and so the tension in these confrontations can quickly escalate. At the least, this situation is awkward and embarrassing; in other situations, it could lead to disruptive or even more dangerous behavior.

Unfortunately, under current CTR standards, structuring is often inferred from conduct rather than any hard evidence of money laundering. Therefore, individuals are reported who have absolutely no connection to otherwise illicit activity—especially not to any financial crime that threatens the banking system or our national security. Most structuring SARs are filed based on technical requirements rather than any concern that a serious criminal enterprise is underway. Yet approaching individuals based on SARs for which agents do not obtain (from the bank or other sources) any indicia of serious money laundering or terrorism financing often results in effectively identifying the bank's SAR filing. This identification needlessly threatens banking relationships and consumes law enforcement resources that could surely be better applied to cases of greater importance to the fight against terrorism financing or organized crime.

ABA urges IRS-CID and those with similar programs to reconsider their approach to investigating structuring SARs. We believe that FinCEN and the bank regulators should work with law enforcement to devise best practices that would better honor the letter and spirit of the SAR safe harbor and make superior use of investigative resources. To the extent that the IRS-CID approach has an "education" value for the individual confronted, we believe that by compromising the SAR safe harbor, it comes at too high a price. ABA and its members are prepared to work with the IRS, FinCEN, the banking regulators, and other interested parties in developing a communication strategy that will better educate bank customers about the BSA data reporting process and more effectively discourage idiosyncratic structuring behavior without jeopardizing SAR confidentiality.

Conclusion

Entering the second decade of expanded SAR filing, it is time to apply the lessons learned about all forms of BSA data reporting to improve the process, to give priority to the reports that have the highest value to law enforcement, and to eliminate the burden on banks for those reports that do not contribute such value. In this way, all parties can apply their scarce resources more effectively to the important mission of combating terrorism financing, money laundering and serious financial crime that can threaten our national security and the integrity of the American banking system.

ABA has always had a strong commitment to BSA compliance and has devoted considerable resources to informing and educating banks on compliance requirements. ABA provides valuable support to the frontline efforts of our bankers. For example, ABA produces a bi-monthly electronic newsletter on money laundering and terrorist financing issues, offers online training on BSA compliance, and has a standing committee of more than 80 bankers who have AML responsibilities within their institutions that help us inform our policy positions and improve our outreach efforts. This year, ABA will once again hold our annual conference with the American Bar Association on money laundering enforcement that is approaching its 20th anniversary, and which has educated thousands of people who are enlisted in this important effort. We will continue to apply our resources, as well as our analysis and our advocacy efforts, to the task of helping to build a financial crime deterrence, detection and enforcement program that sheds outdated obligations in favor of more efficient methods.

Thank you for your attention to these issues. I would be happy to answer any questions.

FINANCIAL SERVICE CENTERS OF AMERICA, INC.
A NATIONAL TRADE ASSOCIATION

Statement of

SCOTT K. McCLAIN
Deputy General Counsel

Financial Service Centers of America

Before the
U. S. House Committee on Financial Services
Subcommittee on Oversight and Investigations

Regarding
Suspicious Activity and Currency Transaction Reports:
Balancing Law Enforcement Utility and Regulatory Requirements

Washington, D.C.

May 10, 2007

www.FISCA.ORG

NATIONAL HEADQUARTERS: COURT PLAZA SOUTH, EAST WING • 21 MAIN ST •PO BOX 647 •HACKENSACK, NJ 07602 •TEL. 201-487-0412 • FAX 201-487-3954
WASHINGTON, D.C. OFFICE: 1730 M STREET N.W. • SUITE 200 • WASHINGTON, D.C. 20036 • TEL. 202-296-3522 • FAX 202-296-7713

Chairman Watt, Ranking Member Miller, and esteemed Members of the Subcommittee, my name is Scott McClain. I serve as Deputy General Counsel to the Financial Service Centers of America, also known as FiSCA. On behalf of the FiSCA membership, I am grateful for the opportunity to appear today to discuss Suspicious Activities and Currency Transaction Reporting by the community financial services industry, and the regulatory burdens on this industry resulting from the current CTR/SAR reporting regime.

FiSCA is a national trade association representing over 6,000 neighborhood financial service providers operating throughout the United States. Our members are classified under the Bank Secrecy Act ("BSA") as "money services businesses" or "MSBs," and as such are subject to stringent federal anti-money laundering reporting and recordkeeping requirements. By way of introduction, our membership is comprised of community-based financial institutions, which serve millions of customers from all walks of life, including those with bank accounts as well as the "unbanked." Our members provide a range of financial services and products, including check cashing, remittances, money order sales, and utility bill payment services, to name a few. Our industry includes large, publicly traded entities operating thousands of locations, down to corner grocery store "mom and pop" establishments offering ancillary financial services.

The success of the community financial services industry is a direct result of its ability to respond to the needs of our customers; in this regard we specialize in delivering three basic commodities that today's consumers need with regard to their finances: convenience, liquidity and choice. The marketplace has shown us that check cashers and other MSBs are best positioned to deliver these features to our customers; a recent national FiSCA survey found that 97% of our customers rate our services from "excellent" to "good."

The MSB industry is not a "shadow economy" operating on some imaginary parallel track with more traditional financial institutions, and serving a separate consumer base. We serve the working men and women of this country in the communities in which they live – and we are very much a part of the mainstream of a vibrant national economy.

FiSCA and its members have committed significant resources in the fight against money laundering and financial crime. As an industry, we recognize the need for strict adherence to BSA compliance requirements, and the need for comprehensive education of MSB personnel. Some of our compliance initiatives have included development of specialized industry guidance materials and manuals, creation of Internet-based compliance courses, and issuance of model compliance policies and procedures to assist the industry in meeting requirements under the USA PATRIOT Act. Additionally, FiSCA hosts an annual conference, where we offer seminars, workshops and materials on BSA compliance.

FiSCA and its members continue to work with FinCEN and IRS, as well as our

state regulators, in reaching out to the broader community financial services industry, and in supporting an effective and rational national anti-money laundering strategy.

Mr. Chairman, in accordance with your May 3, 2007 letter, you have invited us to address the regulatory and cost requirements to financial institutions with regard to current SAR and CTR regulations, and their impact on the community financial services industry. We are grateful for this opportunity to make the following general observations and recommendations:

1. Information generated from SARs and CTRs is reported to be valuable to the goals of law enforcement in combating money laundering and financial crime. Clearly, however, regulatory pressures and the lack of clear guidance in this area have resulted in a tremendous number of defensive SAR filings, and duplicative CTR filings, at a tremendous cost to industry. Critical analysis of the efficacy of the current SAR and CTR regulatory framework, and its impact on the MSB industry, is needed.

2. Increased compliance, transaction monitoring and operational costs associated with SARs and CTRs have significantly burdened the MSB industry, as well as the banks that serve us. These growing costs translate into a downward pressure to increase transaction fees charged to our customers in order to sustain existing revenue levels. In those states where MSB transaction fees are governed by statute, MSBs are caught in a vice and must find other means of covering these expenses. The value of SAR and CTR information to law enforcement should be weighed against its cost to the MSB industry and consumers.

3. MSBs provide critical financial services in communities across the U.S., and provide an infrastructure for remittance flows that support economies in many countries. An unintended consequence of the federal anti-money laundering policy has been a trend among banks and other depositories to terminate their MSB customers. This trend threatens the legitimate MSB industry, and may ultimately cause MSB customer transactions to migrate to untraceable channels. In the interests of federal anti-money laundering policy, depositories should be relieved of excess regulatory burdens applicable to serving the MSB industry.

Regulation of the MSB Industry

The community financial services industry is regulated on both the federal and state levels, and is subject to many of the same types of reporting and recordkeeping requirements as banks and other depositories. Money services businesses, as that term is defined under the Bank Secrecy Act, include check cashers, money transmitters and their agents, issuers and sellers of money orders, traveler's checks and other monetary instruments, currency dealers and exchangers, and issuers and sellers "stored value" products such as prepaid debit and gift cards.

In accordance with provisions of the USA PATRIOT Act of 2001, most types of MSBs are required to register with the Department of the Treasury, and renew their

registration status on a bi-annual basis. As of April 4, 2007, more than 36,000 companies were listed on FinCEN's public database of registered MSBs.

In accordance with Section 352 of the USA PATRIOT Act, all MSBs, regardless of size or location, are required to maintain 4-part anti-money laundering compliance programs, including written policies and procedures, appointment of compliance officers, employee training programs, and periodic independent examinations to ensure that anti-money laundering programs are properly and effectively administered. These systems must be specifically tailored to address the unique risk profile of each individual company, and the financial products and services that each provides.

As federally regulated financial institutions, MSBs are subject to rigorous compliance examinations by Internal Revenue Service agents. In a typical BSA examination, the IRS examiner will focus on key areas to ensure that the company's written policies and procedures are appropriate, that employees are properly trained, that the company has adequate cash controls, and controls for appropriate SAR and CTR reporting. In our view, IRS has done exceptionally well in identifying MSBs for examination, and in executing its overall MSB examination strategy. In larger metropolitan centers, virtually all licensed money transmitters and check cashers have been examined, and many have been the subject of multiple examinations. Moreover, IRS's educational outreach to the MSB industry has been exceptional.

A significant and growing number of state banking agencies also regulate their check cashers and money transmitters, including compliance with State and federal anti-money laundering requirements. Some states subject their MSB licensees to rigorous periodic inspection by state bank examiners. As a result of the recent "Memoranda of Understanding" between FinCEN and various state agencies, a process is now in place to permit information sharing between the state authorities and the federal government on MSB examinations. The Money Transmitter Regulators Association, which is made up of MSB regulators from across the U.S., has also worked with the MSB industry to promote industry-wide compliance.

Contrary to the perceptions of some, the MSB industry's record of compliance with the BSA is quite good. As noted by IRS Fraud/Bank Secrecy Act Director Eileen Meyer in her September 12, 2006 testimony before the Senate Committee on Banking, Housing and Urban Affairs, in the first 8 months of 2006, IRS had conducted examinations of 5,481 MSBs, which resulted in only 17 referrals to FinCEN for potential administrative action, and 14 referrals to IRS-CI for further criminal investigation. That translates into a referral rate of approximately .57%, of which only a handful will result in actual administrative action or criminal conviction.

With respect to the check cashing industry, in particular, since April 1999, FinCEN has assessed a total of $360,500 in civil penalties against check cashers for BSA violations – yet during the same period it assessed well over $60,000,000 against banks and other financial institutions. Since 9/11, only two check cashers have been cited by FinCEN for BSA violations, resulting in civil penalties of only $35,000. Citing

recent examples, BSA violations involving depositories frequently involve tens of millions of dollars. Moreover, since the passage of the USA PATRIOT Act, IRS has dramatically increased the number and scope of BSA examinations of check cashers. Nonetheless, there has not been a corresponding increase in BSA violations found within the check cashing industry.

In short, although the MSB industry is often regarded with suspicion by federal bank regulators who may not fully understand this market sector, when viewed with the "more traditional" banking industry, the record reveals that MSBs truly measure up.

Suspicious Activities and Currency Transaction Reporting Requirements

SAR and CTR filing requirements are the cornerstones of U.S. financial crime enforcement strategy. As the main anti-money laundering weapons in our federal arsenal, it is important that their efficacy to law enforcement be critically evaluated to ensure that they are indeed generating the most valuable data possible.

The threshold dollar amount for MSB SAR filing is $2,000, whereas depositories must file at the $5,000 level. MSBs are required to file SARs (FinCEN Form 109) for transactions of $2,000 or more that are suspected of involving money laundering or other crimes. SARs are required in any instances where the MSB suspects that the funds involved in the transaction are derived from illegal activity or are being used for a criminal purpose, or where the transaction has no legitimate business purpose or is designed to evade a reporting requirement (e.g., a CTR filing). SARs are not limited to hard currency transactions; any suspicious use of funds transfers, monetary instruments or currency exchange should be reported. Although SARs are not mandatory in connection with check cashing transactions, check cashers may file SARs on a voluntary basis, and still enjoy the benefit of certain "safe harbor" provisions of the BSA.

MSBs have only been required to file SARs since April 13, 2000. As evident from figures published by FinCEN, the MSB industry has embraced its regulatory responsibilities in this area. During the first 6 months of 2006, MSBs filed some 270,718 SARs across the broad spectrum of MSB products and services. During this same period, banks and depositories filed 279,703 SARs.

With regard to Currency Transaction Reports, MSBs must file CTRs (FinCEN Form 104) on each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000," conducted by or on behalf of the same person during the same business day. Examples of reportable transactions would include customer purchases of money orders, funds transfer requests, or check cashing transactions in excess of $10,000.

In fiscal year 2006, U.S. financial institutions, including banks and MSBs, filed nearly 16 million CTRs. As previously reported by FinCEN, it is suspected that as many as 30% of CTR filings are repeat filings on routine customer transactions. These

requirements create significant filing and recordkeeping burdens on MSBs and other financial institutions. Moreover, all of the data generated by these filings place significant demands on the federal government to ensure that the information is properly processed and analyzed, and that the information remains secure.

Direct Cost Factors

SAR and CTR compliance requirements have resulted in direct and substantial costs across the financial services landscape, including the MSB industry. Our members have identified Bank Secrecy Act compliance as among the largest costs facing community financial service providers. Generally, these costs are experienced in several key areas including increased labor, information technology costs, professional and service fees, and banking service charges.

With respect to the labor component, MSBs are required to train employees with regard to SAR and CTR requirements, including dollar thresholds, customer identification requirements, and identification of reportable transactions. Training must be provided on an ongoing basis. Moreover, MSBs are required to designate specific compliance officer personnel who are charged with the responsibility of ensuring that suspicious activities are investigated and documented, and that SAR and CTR reporting is accurate and completed in a timely manner. These requirements not only place more responsibilities on individual employees, but it also distracts them from their primary role in serving customers. These added duties must be satisfied either by hiring additional personnel, or expanding roles of existing personnel, both of which result in additional operational costs to MSBs.

Broken down, the man-hour driven component of compliance includes: (a) the development and maintenance of written policies and procedures (in the areas of customer identification, filing reports, creating and retaining records, and responding to law enforcement requests); (b) appointment of compliance officers to oversee compliance programs on an ongoing basis; (c) development and implementation of employee training programs, including written training materials, initial and ongoing training and testing; and (d) periodic independent reviews of compliance programs by qualified examiners to ensure that programs are properly administered.

The increase in information technology costs has been very significant. In an effort to meet ever increasing compliance requirements, a growing number of MSBs have been required to implement costly information systems designed to isolate reportable transactions, create and track customer transaction histories, and generate and store filed CTR and SAR information. Although estimates vary by financial institution, these costs have increased across the board. MSBs with multiple agents or branches are being required to implement advanced systems that have the ability to aggregate transaction information generated from different locations. As a result of BSA requirements that all records be maintained for at least 5 years, electronic data storage costs have also become a significant cost factor. Smaller MSBs, who have felt

the pressure to adopt information systems in order to meet ever increasing compliance responsibilities, have been particularly hard-hit.

Another significant cost factor has been in the area of increased professional and service fees to MSBs. BSA regulations require that MSBs must be subjected to periodic, independent examinations of compliance programs and systems to ensure that they are properly functioning. Frequently, MSBs look to outside experts and consultants to perform this highly specialized function. In many instances, MSBs are required by their depository institutions to retain counsel or outside compliance specialists as a condition of maintaining account relationships. On-site compliance audits and reporting, which is typically performed on an annual basis, can run from $1,000 per location into the tens of thousands of dollars, depending on the size and nature of the MSB.

Banks that service MSBs have likewise experienced mounting compliance and account monitoring costs associated with BSA requirements. Typically, these additional compliance costs are passed on to the bank's MSB customers in the form of increased service fees and charges. One FiSCA member reported that its bank now charges a "monthly compliance monitoring fee" of $2,000 in addition to all regular banking charges for each MSB account. Other FiSCA members have reported that their banks have tacked on flat monthly monitoring fees ranging from a few hundred to a few thousand dollars, regardless of actual account activity. Banking fees for MSBs have increased significantly since enactment of the USA PATRIOT Act.

Clearly, increased compliance and operational costs associated with SARs and CTRs have significantly burdened the MSB industry, as well as the banks that serve us. Studies by state MSB associations have demonstrated that these growing costs translate into a downward pressure to increase transaction fees charged to MSB customers in order to sustain existing revenue levels. In states where MSB transaction fees are governed by statute, MSBs are caught in a vice and must find other means of absorbing these expenses. Unlike depositories or other commercial enterprises, fee-regulated MSB's do not have the option to pass along increased regulatory compliance costs to the consumer.

In sum, MSBs truly bear the cost of our national BSA enforcement strategy. The MSB sector has been given little to no relief from the cost burden associated with their SAR and CTR compliance measures. Any analysis of the value of SAR and CTR information to law enforcement should take into account its cost to the MSB industry.

Defensive SAR Filings

It is common knowledge that following the events of 9/11 and implementation of USA PATRIOT Act, there has been a tremendous increase in regulatory scrutiny of the financial services industry. Across the board, all sectors of the financial services industry have responded to these pressures by engaging in a practice of defensive SAR filings. MSBs are persuaded that the key to avoiding sanctions under the BSA is to file reports on transactions involving even marginally irregular activity. As a result, FinCEN

and law enforcement agencies are deluged with and must process reports that are of dubious value. The information that these reports generate is largely useless, or worse, may serve to obfuscate otherwise valuable direct and statistical data.

We have seen that the pressure towards defensive filings emanates in many cases from field-level examiners who "second guess" decisions by compliance personnel. Our members have reported examples where examiners have been critical of MSBs who had not filed enough SARs, and examples where MSBs have been cited for not filing SARs on transactions that they knew to have a legitimate purpose. In response, rather than scrutinize and investigate anomalous customer activity (with the possibility of uncovering truly valuable information) MSBs and other financial institutions are adopting a "when in doubt, fill it out" philosophy and are filing simply to cover their backs.

The MSB industry has not been provided information as to the value SARs actually have to law enforcement. We have no sense as to the number of reports that lead to criminal investigations, and the number of those investigations that result in money laundering convictions. Without information regarding the actual value these reports serve, the MSBs submitting the reports become disillusioned with the bureaucratic red-tape. The underlying purpose and importance of accurate SAR filings is not communicated to industry, which further encourages defensive SAR filings.

To the extent that field examiners continue to be critical of SAR filing decisions, the trend towards defensive filings will be perpetuated. Clearly, further examiner guidance in this area is required.

Additionally, the value of the current $2,000 threshold for MSB reporting of suspicious activities should be reevaluated. Transactions at the $2,000 level are clearly within the realm of normal consumer activity, thus the current threshold should be adjusted upward based on current economic realities.

Need For Adjustment of the CTR Threshold

MSBs file millions of CTRs annually. Unlike depositories, there is no exemption procedure for MSBs permitting them to be relieved of CTR filing obligations on certain designated transactions. As outlined above, the CTR filing process has resulted in significant costs to the community financial services industry and its customers.

FiSCA supports an increase in the reporting threshold for currency transactions. The present $10,000 CTR threshold was established in 1970. Since that time, the threshold has not been increased and has been rendered out-dated due to inflation. Adjusting for inflation, $10,000 as of 1970 would be the equivalent of $52,963 in today's dollars. Considering the current volume of routine business activity in the $10,000 range, a failure to adjust the CTR threshold is causing the reporting system to be clogged with transaction information that is of little practical value to law enforcement.

Although some law enforcement officials have opposed any adjustment of the current CTR threshold due to concerns that valuable data may be lost, the propriety of the current threshold should be evaluated based on prevailing economic realities. An immediate benefit to law enforcement would be a more accurate data system, unburdened with information from millions of normal transactions. Moreover, it should be noted that an increase in the reporting threshold would in no way relieve financial institutions of the responsibility to report structured transactions or other suspicious activity at levels below the CTR threshold.

Bank Account Terminations

In addition to these direct cost factors, the post-9/11 BSA enforcement regime has inadvertently given rise to an indirect, yet very costly burden to the MSB industry: the termination of MSB bank accounts. The emergence of a bank discontinuance problem was initially reported by FiSCA to FinCEN in 2000. Since that time, the industry has seen an increasing trend of banks making wide-scale terminations of their check casher and money transmitter accounts. A growing number of banks presently serving the industry are refusing to open new accounts, or are placing onerous requirements on the accounts they maintain. Any assessment of the utility of SAR and CTR information to law enforcement should also take into account the impact that BSA compliance has had on the MSB industry.

Banks refer to undue regulatory pressure and attendant costs as the primary reason driving MSB account closures. There is no question but that depositories that service MSBs are faced with significant regulatory burdens, and are required to expend ever greater resources in maintaining MSB customer compliance and monitoring systems. Due to this uncertain regulatory environment, many banks have opted to discontinue their check casher and money transmitter customers.

The importance of the domestic MSB industry cannot be underestimated. MSBs provide critical financial services in communities across the U.S., and provide an infrastructure for remittance flows that support economies in many developing countries. Remittance flows from the U.S. to Latin America exceeded $62 billion in 2006. MSBs, by their very nature, are critically dependent on access to depository accounts and banking services in order to conduct business.

Thus far, a regulatory solution has eluded us. The MSB industry as a whole was encouraged by FinCEN's efforts in convening the March 2005 fact-finding hearing, and in spearheading the resulting Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States (the "MSB Guidance"), issued April 26, 2005. Two years later, however, it is clear from reports from our membership that the MSB Guidance has not achieved the purpose of creating greater access to banking services for the industry. Since issuance of the MSB Guidance, there has been a net loss in the overall number banks willing to serve MSBs. We are aware of no major bank which, having previously terminated its MSB customers, has returned to the industry.

Loss of MSB bank accounts threatens to drive MSB customer transactions underground through unregulated channels, including bulk cash smuggling and other means. It is critical to the interests of national security that transparency of MSB transactions be maintained by ensuring that MSBs remain part of the regulated financial community and continue to have access to depository services.

FiSCA supports the introduction of an appropriate legislative solution designed to relieve our banks of excessive regulatory burdens in serving MSBs. Banks should not be expected to serve as the *de facto* regulator of their MSB customers, and should not be called upon to assess the effectiveness of the compliance systems of their MSB customers – a role clearly regulatory in scope.

In this regard, FiSCA has been instrumental in the formation of an MSB Coalition to examine possible solutions to the present accounts termination problem. The MSB Coalition is made up of representatives from all segments of the MSB community, including the check casher industry, money transmitters, money order processors, and others with interests in the MSB community. The goal of the MSB Coalition is to examine possible solutions to the bank discontinuance problem, linked to providing regulatory relief to banks servicing MSBs. The Coalition is reaching out to all members of the MSB community, as well as key state and federal regulatory bodies, in an effort to increase awareness and encourage participation in solutions on this and related issues.

Conclusion

In conclusion, regulatory pressures and the lack of clear guidance in this area have resulted in a tremendous number of defensive SAR filings, and duplicative CTR filings, at a tremendous cost to industry. Existing reporting thresholds should be reevaluated, and the current SAR/CTR reporting system and its cost to the financial services industry should be critically assessed.

The community financial services industry is committed to the ongoing battle against money laundering and terrorist financing. As with other sectors of the U.S. financial system, it is critically important that we protect the integrity and legitimacy of our industry. It is equally critical, however, that the MSB industry be recognized as being a part of a healthy financial industry, and partner in the war on financial crime.

Again, we thank you for the opportunity to present these views.

Testimony of

R. Michael Stewart Menzies, Sr.
President/CEO, Easton Bank and Trust Company

On behalf of the
Independent Community Bankers of America

Before the

Congress of the United States
House of Representatives
Committee on Financial Services
Subcommittee on Oversight and Investigations

Hearing on

"Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements"

May 10, 2007
Washington, D.C.

Chairman Watt, Ranking Member Miller and members of the committee, my name is Mike Menzies. I am President and CEO of Easton Bank and Trust Company in Easton, Maryland. I am pleased to testify today in my capacity as Vice Chairman of the Independent Community Bankers of America (ICBA).

On behalf of ICBA's nearly 5000 member banks, I want to express our appreciation for the opportunity to testify about the burdens community banks face when complying with the Bank Secrecy Act.

Summary of ICBA Position

Community bankers are committed to balanced effective measures that stop terrorists from using the financial system to fund their operations and prevent money launderers from hiding the proceeds of criminal activities. However, **ICBA strongly urges the federal government to recognize the costs and burdens that these requirements place on financial institutions, especially community banks, and to find ways to streamline requirements.**

ICBA believes the government should focus on a risk-based approach in combating money laundering and terrorist financing, with a careful balancing of costs and benefits. To that end, **we support the development of a streamlined and easily applied system to exempt "seasoned customers" from currency transaction reports** and we applaud the House for once again passing H. R. 323 that would implement a seasoned customer exemption.

H. R. 323 is substantially similar to section 202 of Representative Nydia Velazquez's Communities First Act, H. R. 1869, which ICBA strongly supports. That legislation provides critical regulatory and tax relief to community banks and their customers. We urge this committee to carefully consider each of the regulatory provisions of that bill as potential additions to your agenda this year.

In addition, our testimony includes the following recommendations:

- FinCEN needs sufficient resources to manage the data
- Law enforcement should clearly demonstrate the usefulness of the data
- A simple increase in the threshold for CTRs would greatly reduce burden
- The streamlined exemption process in H. R. 323 will help restore the balance between costs and benefits
- BSA requirements should be flexible and easily applied
- Enhanced communication between law enforcement, regulators and banks is extremely important
- Community banks need regulatory relief

Expanding Burden and Reporting

When it initially adopted the Bank Secrecy Act in 1970, the United States Congress determined that "certain records maintained by businesses... have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings."[1] As a result, community banks were required to maintain "appropriate types of records and the making of appropriate reports."[2]

Over the years, the requirements – and burdens – imposed on community banks under the Bank Secrecy Act have steadily increased. Most recently, in 2001 after the terrorist attacks on New York and the Pentagon, Congress expanded the requirements again in the USA PATRIOT Act, broadening the definition of financial institution to encompass many additional businesses and increasing the requirements for banks and other financial institutions.

As a result, the volume of reports that have been filed under the BSA has been increasing dramatically. According to the Treasury's Financial Crimes Enforcement Network, or FinCEN, the number of suspicious activity reports, or SARs, that banks filed in 1996 was 62,388; by 2000, that number had nearly tripled to 162,720 and in 2005, the last year FinCEN reported a complete year of figures, the number reached over one-half million suspicious activity reports.[3] The number of currency transaction reports (CTRs) has also been increasing – reaching nearly 16 million in 2006.[4]

FinCEN Needs Sufficient Resources to Handle the Data

Before addressing the burden on the nation's community banks, it is important to recognize that sufficient resources are needed to make the information that banks supply truly useful. Unless FinCEN has sufficient resources to be able to make the data worthwhile, it does not make sense to ask banks to file the many reports currently required. Merely collecting the data and tabulating it in a database does not achieve the goal of combating money laundering and terrorist financing. Rather, it is important that FinCEN has the resources and funding to hire sufficient staff to analyze the data and to develop and implement software programs that can monitor the data while fulfilling FinCEN's broader law enforcement mission. FinCEN is not a large organization but since 2001 it has been given increasing responsibility. To handle these responsibilities, especially all the reports banks produce, FinCEN must have the funding it needs.

Insufficient funding is having an impact. For example, last July, FinCEN announced it had stopped work on the BSA Direct Retrieval and Sharing Component project because it had repeatedly missed program milestones and

---

[1] 12 USC 1951. Bank Secrecy Act § 121 (84 Stat. 1116).
[2] Ibid.
[3] *The SAR Activity Review, By the Numbers, Issue 7, November 2006.*
[4] *FinCEN Annual Report for Fiscal Year 2006*, page 11.

performance objectives.[5] The agency's press release stated that, "The level of effort and costs to complete BSA Direct R&S, address all remaining defects of the system, and operate and maintain the system, [were] likely to be much greater than originally projected."[6] At the time it ceased work, $14.4 million had been spent, $5.5 million more than originally projected with an additional $8 million needed before the system could be completed and an additional $2.5 million per year for operations and maintenance.[7] Difficulty in collecting and managing BSA data is ongoing. Recently, FinCEN deferred the effective date of the revised SAR form due to problems with managing the input of data from the new form.[8]

For FinCEN to handle the data that it is statutorily obligated to manage, Congress needs to allocate additional funds. Looking forward, as FinCEN manages more data, it will need more funding and analytical resources to make the continued collection of data worthwhile. With more industries filing reports, the demand for resources and funding to analyze the date properly will only increase.

Use of the Data

Not only FinCEN, but law enforcement agencies need sufficient resources to be able to benefit from the data that FinCEN processes. Perhaps one indicator of how the data that banks produce is used by law enforcement agencies can be found in a regular report issued by FinCEN. It's also worth considering the relationship between banks and law enforcement in assessing this process.

Under the USA PATRIOT Act section 314(a),[9] banks are required to review their records to ascertain whether there is a data match corresponding to a request from a federal law enforcement agency. As of April 24, 2007, according to FinCEN's own fact sheet, this provision allows law enforcement "to reach out to more than 45,000 points of contact at more than 27,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering."[10] Every two weeks, FinCEN transmits a request to banks to search records for data matches, including accounts maintained by the subjects listed in the request. There is no obligation to respond if there is no match. Just after the program initially started, it had to be temporarily suspended because of problems and security concerns over the data transmissions. However, it has since resumed.
It's worth noting that many wrongly assume that these compulsory data searches are automated. For larger institutions, that may be true to some extent.

---

[5] FinCEN press release, July 13, 2006.
[6] Ibid.
[7] Ibid.
[8] *Federal Register,* volume 72, no. 83, May 1, 2007, page 23891.
[9] 31 USC 5311.
[10] FinCEN's 314(a) Fact Sheet, April 24, 2007.

However, we understand that even larger banks have to subject their records to manual processes as well. While the costs for software and automated processing are decreasing, smaller banks do not always have the resources to install the necessary software. As a result, many banks - especially community banks – still must conduct intensive and time consuming manual searches of their records to determine whether there is a match to the FinCEN list. Bear in mind, these searches must be completed immediately because the statute requires the bank to respond within two weeks.

According to FinCEN, from November 2002 until April 24 of this year, banks were asked to search their records for data matches for nearly 5,500 subjects. That means someone in the bank has to review account records in different data systems, including deposit records, consumer loan records, commercial loan records, pension accounts records, trust account records, and other systems in the bank. While software producers would like us to believe that banks have quick and easy customer information programs that allow all these databases to talk with one another, the average bank software does not have the advanced capability to do so. Manual data searches are time-consuming and use resources that the bank might otherwise devote to serving its customers. FinCEN has been working with the industry to focus the requests and to eliminate the need to search records when there is little chance of finding a positive match. Regardless of these efforts, the time needed to respond to these search requests is a substantial burden.

Ultimately, the effectiveness of a program must be judged on its results. After years of broad compliance with BSA bank record searches at a substantial cost to the banking industry, FinCEN reports that the data-match program has led to just under 1,500 grand jury subpoenas, 21 search warrants, 100 arrests, 112 indictments and 9 convictions.[11]

The Burden of Bank Secrecy Act Compliance

As noted above, the nation's community banks are committed to supporting the federal government's efforts to prevent money laundering, terrorist financing and other fraudulent activities. However, ICBA believes that it is critical that resources be focused where the risks are greatest. Over the years, there has been a tendency to require reports that have little value for law enforcement because it *might* be useful. However, these reports merely clog the system and obscure truly suspicious activities. Moreover, all this data places additional demands on the federal government to properly process and analyze the information – and to ensure that it is properly protected in a secure electronic database. Committees in each house of Congress are currently focusing on data security and as part of that process, it is critical that the federal government ensure that the vast amount of sensitive BSA data is properly protected. Every day, there are stories in the media about identity theft and the risks to

[11] FinCEN's 314(a) Fact Sheet, April 24, 2007.

consumers. We cannot overlook the need to secure and protect the large amount of data collected by the government under BSA requirements.

Bankers across the country continue to identify the Bank Secrecy Act as the most burdensome area of compliance. The time it takes for banks to develop systems and procedures, train personnel, audit for compliance, and take the many other steps needed to comply with the many requirements and reports mandated by the BSA are time consuming.

Therefore, ICBA appreciates the efforts by Congress to bring greater focus to this issue and we look forward to continuing to work with Congress, the Treasury and the banking agencies to achieve an effective compliance regime that directs resources to banks, regulators and law enforcement agencies where it can be of the most benefit. For example, one solution ICBA strongly supports is streamlining the process for currency transaction reports (CTRs). H. R. 323 would greatly help streamline the entire reporting process and restore balance to the system of exempting customers from unnecessary CTRs where the current exemption system is not working.

ICBA Supports the "Seasoned Customer Exemption (CTR) Act of 2007"

We applaud this committee and the House for passing H.R. 323. The provisions of the bill are substantially similar to legislation passed by the House last session as part of a comprehensive financial regulatory relief bill. Just as it did last session, the House passed the bill by an overwhelming majority.

As the bill properly notes, "the completion of and filing of currency transaction reports....poses a compliance burden on the industry." Unfortunately, despite these efforts and compliance burdens, the bill also notes that not all the reports are "relevant to the detection, deterrence, or investigation of financial crimes, including money laundering and the financing of terrorism."

ICBA has long advocated developing a simple and easily applied exemption process that can eliminate currency transaction reports that have little value for law enforcement. H.R. 323 that would allow banks to exempt seasoned customers from CTRs without being required to renew the exemption annually. Past efforts to increase the use of the current exemption process have not succeeded, despite years of efforts by interested parties, including industry representatives, regulators and law enforcement.

ICBA supports this committee's efforts and H. R. 323 because they have the potential to eliminate many unnecessary reports that are costly to produce but that offer little or no use for law enforcement. Eliminating unnecessary reporting would result in substantial savings to our banks and increase the time our employees can spend on customers' financial needs. They would also make law enforcement investigation more efficient by eliminating unnecessary data.

The bill offers a definition of which customers would be eligible for this new "seasoned customer" exemption. One of the provisions would require that a customer maintain a deposit account with the bank for at least 12 months. ICBA recommends that the Treasury Department be given some flexibility to shorten this timeframe in appropriate circumstances, as determined by Treasury in consultation with other interested parties, including law enforcement and industry representatives.

Ultimately, though, for this provision to succeed, Treasury will have to develop an exemption process for qualified customers that can be simply and easily applied – in other words, a system that truly works. We look forward to continuing to work closely with this committee, Treasury and banking regulators to find additional solutions to reducing the BSA compliance burden while meeting the needs of law enforcement. We hope today's hearing will improve the chances for this provision to become law since adoption of this important legislation is one step that will help reduce the regulatory burden confronting the nation's community banks.

Increased Threshold for CTRs Would Reduce Burden

Fundamentally, ICBA believes that a simple increase in the dollar threshold for CTRs would be easier to apply. The dollar threshold has not been changed since the Bank Secrecy Act was adopted more than thirty-five years ago. However, we recognize that law enforcement agencies are concerned that such a change might eliminate valuable information for detecting and prosecuting criminal activities, especially as they begin to develop new databases and new technologies that can better use the information diligently supplied by the nation's banks.

ICBA's goal is to find a way to eliminate reports of routine transactions that are costly and burdensome to produce but that provide little use for law enforcement. ICBA has actively participated in many discussions on this issue over a number of years through our representation on Treasury's Bank Secrecy Act Advisory Group and we will continue to pursue a solution through that venue. However, Congressional action will send a strong signal to regulatory agencies and law enforcement that a solution is needed. Community bankers often comment that law enforcement has a tendency to shift costs and burdens to the banking industry. Because it is the industry – and not law enforcement – that bears the costs, there is a tendency to disregard the substantial costs of compliance created by the demands for information. It is vitally important that the costs be assessed against the overall benefits. ICBA believes today's hearings helps bring useful focus to the need for balance.

Why the Current Process Does Not Work

Costs and Burdens Associated with the Current Currency Transaction Reporting (CTR) Process. Many financial institutions report that the cost of using the current exemption process outweighs any associated benefits. As a result, many institutions find it is much simpler and less risky to file a CTR on every cash transaction over $10,000. Our members report that this approach is more practical and cost effective than using the exemption process.

Compliance Responsibility. Using the existing BSA exemption not only consumes a community bank's limited resources in time and money, it also increases the burden on the bank's existing compliance program by requiring the bank to develop policies and procedures for exempting customers, train personnel on the procedures, educate customers on the exemption process, and establish audit programs to monitor compliance with the exemption process.

For example, if a community bank establishes an exemption for a customer under current rules, it must document the decision and re-file an exemption with the government every other year. When refilling, the bank must verify it has conducted an annual review of the account for compliance with the exemption. It then must ensure: (1) that it has up-to-date exemption lists available for all branch personnel; (2) that all branch personnel are properly trained in which customers are exempt; and (3) that all employees know when exemptions can be used because not all transactions for an exempt customer may be exempt.

Resource Allocation. For many institutions, particularly community banks, implementing exemptions under the current rules is not cost effective. Many community banks lack the time or resources to study the exemption requirements and how they would apply to specific customers. Under the current system, it is not only a matter of exempting a customer, but the regulatory burden continues since the bank must continue to monitor exempted accounts and must certify that a customer continues to meet the regulation's exemption criteria. This is especially true for community banks that file a small number of CTRs. For these institutions, simply filing on all cash transactions over $10,000 is a more efficient means of allocating precious compliance resources. Instituting simpler procedures could make the process more cost effective and reduce the risk of compliance violations.

With high turnover of tellers and other branch staff, it is often simpler, less complicated and less confusing simply to train all staff to file the currency report for every cash transaction over $10,000. This policy is plain, simple and easily applied. Unfortunately, it also means many routine transactions are reported.

The advantages of not using the exemption process are that the bank will not mistakenly exempt a transaction that should be reported, and the bank can avoid a portion of the BSA audit and related regulator scrutiny. In other words, the

costs for the current process and the risks associated with using it have caused most bankers – especially community bankers – to conclude the exemption merely creates costs and increases risks.

Automation. Where feasible and within a bank's budget, many larger institutions that file CTRs on every transaction above the $10,000 threshold have elected to automate the reporting process. While cost-prohibitive for many smaller institutions, automated filing systems maximize efficiency by reducing the time that staff must devote to the filing process. Some automated systems automatically generate a CTR for transactions above the $10,000 threshold. Other systems flag transactions for further review by staff. Moreover, since banks must aggregate a customer's transactions in order to properly report currency transactions, automated systems facilitate compliance with the aggregation requirements. However, where banks do rely on automation, it facilitates filing over not filing.

And, it is much more difficult to automate the CTR process if a bank attempts to include exemptions since it requires customization of software systems. Unfortunately, demands on bank technology systems is increasing, not just for BSA compliance, but also provisions under the Fair and Accurate Credit Transactions Act, data security demands, fraud detection and new payment systems technologies such as image processing. As a result, many community banks have concluded it is not cost effective to expend limited resources automating a process fraught with regulatory risk for little benefit.

Suspicious Activity Reporting

Suspicious activity reports, or SARs, are another key element in the entire BSA scheme. ICBA believes that these reports can provide important information. However, it is not always a simple matter to identify activities which may be suspicious. The demands placed on banks to monitor all customer transactions for possible suspicious activities can be time consuming and expensive. Being deputized as law enforcement agents is not a business the banking industry was designed to handle. Banks can and do report activities when they detect something out of the ordinary that cannot be explained. But the requirements are turning into demands that banks closely scrutinize each and every transaction. At one time, there were concerns that banks could be criticized for failing to file a SAR, and there were rumors that regulators had a "zero tolerance" for violations. In part, these rumors were fueled by heavy sanctions imposed on Riggs National Bank, AmSouth and other financial institutions. Examiners in the field also fed the fire with requirements that banks be compared to their peers with respect to the number of SARs being filed and that banks be prepared to fully document and explain and changes in the level of SARs being filed.

Fortunately, the interagency Bank Secrecy Act/Anti-Money Laundering Examination manual issued in 2005 helped address many of these problems,

and the requirements for SAR filing are much better understood by bankers and examiners. However, as with any regulatory requirement, this is an ongoing process and there are still lingering elements of "defensive filing" of SARs. This is diminishing, but many community banks across the country feel it is better to go ahead and file rather than risk examiner criticism. Continuing communication and guidance from regulators to banks – and examiners – will help. This is one of the reasons ICBA so strongly believes that enhanced communication from regulators and law enforcement is critical.

Bank Secrecy Act (BSA) Requirements Should Be Flexible and Easily Applied

To begin to address some of these burdens, ICBA encourages the federal government to continue working with the banking industry to provide additional guidance—such as best practices, questions and answers, or commentary—that is understandable, workable and easily applied by community banks. Overall, the BSA/AML Exam Manual and the subsequent outreach sessions to industry and examiners, where the industry and regulators worked together, are an excellent model. These efforts, in which ICBA played a key part, have helped to greatly reduce some of the BSA compliance burdens faced by community banks. Since cooperation between the government and financial institutions in a true working partnership is vital to stop terrorism and money laundering, ICBA urges the government to expand and enhance communications to alert bankers to fact patterns and practices that may be indicative of money laundering or terrorist financing.

BSA Reporting Should Be Simplified and Focus on Truly Suspect Activities. As the government continues to combat money laundering and terrorist financing, it is important to focus on quality over quantity for all BSA reporting. This is one reason ICBA strongly supports efforts to streamline the process to allow community banks to exempt "seasoned customers" from currency transaction reports (CTRs) so that routine transactions are not reported.

More and more data may not always be beneficial, and ICBA encourages Congress and regulators to recognize this in other areas, too. For example, ICBA is concerned that changes to recordkeeping and reporting for routine wire transfers could impose burdens and costs that far outweigh potential benefits to law enforcement. Law enforcement and the federal government must clearly demonstrate the benefits and usefulness of any new data collection and reporting. And, where unnecessary data is being collected, steps should be taken to eliminate those requirements.

Increased Communication Between Government and Banks

ICBA believes it would be helpful to community banks' efforts against money laundering and terrorist financing if they received better information from law

enforcement about what activities to watch for. Under section 314 of the USA PATRIOT Act, noted above, Congress included a provision designed to encourage law enforcement to enhance communication with financial institutions to improve the banking sector's focus on those transactions that present the greatest risk of money laundering or terrorist financing. Through Treasury's Financial Crimes Enforcement Network's *SAR Activity Review,* law enforcement has been steadily – if slowly - increasing the information it provides banks. ICBA encourages Congress to continue to take steps to ensure that this information is provided by law enforcement agencies. An open dialogue between law enforcement and the industry would help community banks focus efforts where they are the most effective. Fundamentally, though, greater information from law enforcement would help banks identify suspicious transactions – and would encourage banks by helping them know their efforts are worthwhile.

Community Banks Need Regulatory Relief

Regulatory burden, including the burdens and costs associated with unnecessary reporting, is crushing community banks and leading many to merge with other institutions in order to handle the ever-increasing compliance requirements. Regulatory burden relief is important to community banks and our customers because community banks' survival depends on the economic vitality of our communities just as the economic vitality of our communities depends on the local community banks. Community bankers provide tremendous leadership which is critical to local economic development and community revitalization.

Community banks are particularly attuned to the needs of small businesses, our nation's engine for job creation. They are the leading suppliers of credit to small businesses and account for a disproportionate share of total lending to small business. Banks with less than $1 billion in assets hold only 13 percent of bank industry assets. However, they are responsible for 37 percent of bank loans small business loans and 64 percent of bank loans to farms.

ICBA supports a bank regulatory system that fosters the safety and soundness of our nation's banking system. However, statutory and regulatory changes continually increase the cumulative regulatory burden for community banks. In recent years, community banks have been saddled with the privacy rules of the Gramm-Leach-Bliley Act, the customer identification rules and anti-money laundering/anti-terrorist financing provisions of the USA Patriot Act, and the accounting, auditing and corporate governance reforms of the Sarbanes-Oxley Act. When viewed in the aggregate, the regulation creates a substantial and disproportionate burden on community bank. In particular, the provisions of the BSA are especially time consuming and burdensome.

This disproportionate impact of the ever-mounting regulatory burden is significantly affecting community banks.[12] Since 1992, the market share of community banks with less than $1 billion in assets has dropped from approximately 20 percent of overall banking assets to 13 percent. During the same period, the market share of large banks with over $25 billion in assets grew from approximately 50 percent to 70 percent.

It is true that the banking industry as a whole has reported record profits in recent years. However, that good fortune is not shared equally. According to the most recent FDIC Quarterly Banking Profile, banks with over $10 billion in assets do much better in most performance ratios than banks with under $100 million in assets.[13] For example, according to the FDIC, the return on assets at banks with over $10 billion in assets at year-end 2006 was 1.32%. For banks in the $1 billion to $10 billion range, that performance ratio declined to 1.22%. For banks in the $100 million to $1 billion range, the return on assets declined still further to 1.17%. And for banks in the under $100 million asset-size category, their return on assets was only 0.93%. Many community banks report that the burden of compliance with laws and regulations – including BSA compliance – erodes their profitability. These figures help to demonstrate that compliance falls more heavily – and is more costly – for smaller institutions.

With smaller customer and asset bases over which to distribute compliance costs, the proportionate cost of compliance with all laws and regulations – including BSA – is also much higher at community banks. This regulatory burden affects the viability of local community banks – and the amount of funds these banks have to reinvest in their local communities through loans and other activities. For example, an analysis of banking trends conducted by two economists at the Federal Reserve Bank of Dallas concluded that the competitive position and future viability of small banks is at risk. The authors suggest that the regulatory environment has evolved to the point of placing small banks at an disadvantage to the detriment of their primary customers: small business, consumers and the agricultural community.

Larger banks also may have hundreds or thousands of employees to handle the many complications of regulatory demands. However, a community bank with $100 million in assets typically has just 30 fulltime employees while a $200 million bank may have about 60 employees in total. If the bank is faced with a new regulation, it must train one or more current employees to take on added responsibilities. This burden not only places more responsibility on the employee, but also distracts them from their primary duty of serving customers. Unlike larger institutions, the typical community bank cannot merely hire a new employee and pass the costs on to its customers.

---

[12] Gunther and Moore, "Small Banks' Competitors Loom Large," *Southwest Economy*, Federal Reserve Bank of Dallas, Jan./Feb. 2004.
[13] FDIC, *Quarterly Banking Profile,* Fourth Quarter 2006.

Conclusion

Specific data is not available that compares the cost of filing CTRs on all transactions above $10,000 to the cost of using the exemptions. In part, because employees at community banks deal with many different issues during the course of the day it is difficult to segregate the costs for individual compliance efforts. However, community banks across the country report that BSA compliance is one of the heavier regulatory burdens to which they have to respond. Adopting H. R. 323 would help alleviate this burden. Anecdotal evidence and comments from financial institutions of all sizes support the notion that avoiding the current exemption process is significantly less burdensome in terms of cost and compliance management. Barring a significant change in the CTR filing process or the exemption regulations, many institutions will continue to file reports on all transactions that exceed the $10,000 threshold as a simple means of complying.

ICBA greatly appreciates this committee's commitment to moving legislation that would reduce the regulatory burden on community banks by clarifying the seasoned customer exemption to the CTR requirement. ICBA looks forward to continuing to work with you in this regard. Thank you.

Testimony of

America's Community Bankers

on

"Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements"

before the

Subcommittee on Oversight and Investigations

of the

Financial Services Committee

of the

United States House of Representatives

on

May 10, 2007

Carolyn M. Mroz
President & CEO
Bay-Vanguard Federal Savings Bank
Baltimore, MD

and

Member, Board of Directors
America's Community Bankers
Washington, DC

Chairman Watt, Ranking Member Miller, and Members of the Subcommittee, I am Carolyn Mroz, President and CEO of Bay-Vanguard Federal Savings Bank in Baltimore, Maryland. Bay-Vanguard Federal Savings Bank is a $134 million depository institution and is a subsidiary of BV Financial, Inc. I am here today representing America's Community Bankers[1] (ACB). I am a member of ACB's Board of Directors, and I serve on ACB's Regulation and Compliance Committee.

We want to thank Chairman Watt for holding this important hearing. Bank Secrecy Act (BSA) compliance is a time-consuming and costly process, and ACB is a strong advocate for regulatory relief in this area. We would also like to thank Chairman Frank and Ranking Member Bachus for their leadership on H.R. 323, the Seasoned Customer CTR Exemption Act of 2007, which was approved by the full House of Representatives earlier this year. This legislation makes important improvements to the current exemption system for Cash Transaction Reports (CTRs) by making it easier to exempt the routine transactions of certain seasoned business customers. We hope that passage of H.R. 323 marks the first step by this Congress towards modernizing the BSA to more appropriately balance the reporting requirements of depository institutions and the information needs of law enforcement agencies.

COMPLIANCE CONCERNS FOR COMMUNITY BANKS

BSA compliance consistently tops the list of the most burdensome regulatory requirements for community bankers. Prior to the terrorist attacks of 9/11, the BSA was primarily a tool for combating drug trafficking and money laundering, a problem most commonly encountered by

[1] America's Community Bankers is the national trade association committed to shaping the future of banking by being the innovative industry leader strengthening the competitive position of community banks. To learn more about ACB, visit www.AmericasCommunityBankers.com

large financial institutions. Today, however, terrorist financing concerns have resulted in a paradigm shift in BSA compliance, and community banks are being held responsible for the same complexity and requirements as multi-national banks, despite differences in their businesses and the fewer resources available to them. ACB supports the goals of these laws; however, inconsistent interpretation of the implementing regulations by examiners and a lack of regulatory guidance have made it increasingly difficult for community banks to comply with anti-money laundering demands and have produced a plethora of unintended consequences.

To illustrate my point, consider an institution like Bay Vanguard, which has $134 million in assets and 31 employees. In addition to serving as President and CEO, I am also our BSA/Compliance Officer. We are a very small bank and our resources do not provide the luxury of a full-time compliance department. For other community banks to comply with these regulations, they must employ a full time senior level BSA officer to manage their BSA compliance responsibilities. The BSA Officer must be a specialist in monitoring and investigating customer transactions, which is a continuous learning process with added costs. Additional bank employees work in concert with our BSA officer to file the Cash Transaction Reports (CTRs) and Suspicious Activity Reports (SARs) with the appropriate regulatory authorities. Because these individuals devote significant time to CTR and SARs, it represents a considerable line item on the bank's operating budget. Because of budget restraints, this takes resources from other areas where the money could be better used, such as hiring additional tellers and loan officers, or funding outreach programs geared towards meeting the convenience and needs of the community. It is important to note that the added payroll and benefit costs, as well as specialized training and continuing education, are a significant burden and expense for

community banks. The training regimen for both new and old employees is on ongoing financial obligation, and third party audits and legal advice for SARs determinations can cost a bank in excess of $25,000 annually. To fully appreciate the financial burden these costs create, you must look at them in the context of a small business. While Congress may be used to approving annual budgets in the billions of dollars, to a community bank, these are real costs that have a great influence on the bank's business decisions and ability to grow.

While there are a number of compliance requirements under the BSA that ACB believes are in need of modernization, today we will limit our testimony to two specific aspects: SARs and CTRs. As the Subcommittee continues its oversight of these monitoring and reporting requirements, we ask that you carefully consider the amount of data banks are required to provide compared to the number of times law enforcement has actually used that data to prosecute terrorism or money laundering. For example, even when law enforcement requests specific information where they may have concerns, FinCEN's 314(a)[2] Fact Sheet dated April 24, 2007 shows that between November 1, 2002 and April 24, 2007, a total of 9 convictions resulted from this unprecedented level of law enforcement investigative authority, as granted through the USA PATRIOT Act. While we are committed to providing the government with the necessary information to combat unlawful and potentially dangerous activities, a greater emphasis should be placed on the quality of data rather than the quantity of data.

---

[2] Section 314(a) of the USA PATRIOT Act of 2001 (P.L. 107-56), required the Secretary of the Treasury to adopt regulations to encourage regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. FinCEN issued a proposed rule on March 5, 2002, and the final rule on September 26, 2002 (67 Fed. Reg. 60,579). Section 314(a) requirements are now published in 31 CFR Part 103.100.

SARs

There is a great deal of research that goes into filing a SAR. The narrative section alone is extremely labor-intensive, and banks are required to describe the suspicious transaction or group of transactions in detailed paragraph form. FinCEN instructs institutions to explain the "5 W's" – who, what, when, where, and why – and institutions are prohibited from attaching accompanying data such as spreadsheets, account records and graphs. The FinCEN exam manual suggests that institutions should be prepared for intense scrutiny of the quality of the narrative by the examiners, which creates added pressure to devote considerable time and resources to the effort.

The federal banking agencies are scrutinizing SARs reporting more closely than ever and anxiety over whether an institution should file a SAR is at an all-time high. As a result, many depository institutions believe that filing more SARs is the key to avoiding regulatory criticism. According to the BSA, banks, bank holding companies, and their subsidiaries are required to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount
- Criminal violations aggregating $5,000 or more when a suspect can be identified
- Criminal violations aggregating $35,000 or more regardless of a potential suspect
- Transactions conducted or attempted through the bank (or affiliate) and aggregating $5,000 or more if the bank (or affiliate) knows, suspects or has reason to suspect that the transaction:
    - May involve money laundering or other illegal activity
    - Is designed to evade BSA requirements
    - Has no business or apparent lawful purpose or is not the type of transaction that the customer would normally be expected to engage in and the bank knows of no reasonable explanation for the transaction after examining available facts

Given these onerous and comprehensive guidelines, many institutions file SARs as a defensive tactic to stave off second guessing of an institution's suspicious activity determinations. This mindset is fueled by examiners who criticize institutions for not filing enough SARs based on their asset size. Furthermore, regulators have admitted in public that the agencies do not discourage the "when in doubt, fill it out" strategy. Enforcement actions appear to confirm the idea that it is better to have filed a SAR when it is not necessary than to have not filed one. Additionally, it is more time consuming and paperwork intensive for an institution to document why it elected not to file a SAR than to simply file the report; this in itself is counterintuitive to the mission and intent of the BSA. Institutions believe that the risk of regulatory criticism is higher for not filing, and examiners will disapprove of the bank's documentation or its decision not to file. Filing a SAR should not be done under fear of regulatory reaction. This undermines the intent of the law and effectively turns the BSA on its head, since the value of SAR data will be less valuable and the integrity and usefulness of the SAR system will be compromised by the onslaught of defensive filing.

In this era of increased regulatory scrutiny, community banks deserve more guidance and information. ACB strongly urges the banking regulators, FinCEN, and the Department of Justice to work to help institutions identify activities that are genuinely suspicious and should be reported. Without additional guidance regarding what events trigger a SAR and what events do not, institutions will ultimately choose a course of action that protects them from a vigorous regulatory environment.

CTRs

FinCEN regulations require financial institutions to file a CTR for all cash transactions over $10,000. Unfortunately, existing CTR laws have departed from the BSA's stated mission of collecting reports and records that "have a high degree of usefulness" for the prosecution and investigation of criminal activity, money laundering, counter-intelligence, and international terrorism. As a result, financial institutions file millions of CTRs each year that provide little or no assistance to law enforcement officials.

On the other hand, FinCEN's regulations establish an exemption system that relieves financial institutions from filing CTRs on the cash transactions of certain entities, provided certain requirements are met. The exemption system was intended to reduce regulatory burden associated with BSA compliance. The exemption process was well intentioned, but community banks have been reluctant to use the exemption system because:

- It is not cost effective for small institutions that do not file many CTRs
- They fear regulatory action in the event that an exemption is used incorrectly
- They lack the time and resources to conduct the research necessary to determine whether a customer is eligible for an exemption and continually monitor the list
- It is easier to automate the process and file a CTR on every transaction that triggers a reporting requirement
- The regulations and the exemption procedures and requirements are overly complex

As a result, FinCEN and law enforcement report that the CTR database is inundated with unhelpful CTRs because financial institutions do not use the exemption procedures that are designed to eliminate CTRs that are of no interest to law enforcement. This ultimately makes it

more difficult to use the database to investigate possible cases of money laundering or terrorist financing.

ACB believes that the BSA should be amended to provide an increase in the dollar value that triggers a CTR filing. The current $10,000 threshold was established in 1970. When adjusted for inflation, $10,000 in 1970 is equivalent to more than $52,925 today[3]. To put it in perspective, the cost of a brand new Corvette in 1970 was approximately $5,000. The cost of a brand new Corvette in 2007 is more than $53,000. We understand that when the regulations were first implemented, there was very little activity over the $10,000 threshold. Today, however, such transactions are routine, particularly for cash-intensive businesses. Raising the threshold does not mean that institutions will be relieved from monitoring account activity for suspicious transactions below the CTR reporting requirement. Increasing the threshold would enable financial institutions to alert law enforcement about activity that is truly suspicious or indicative of money laundering, as opposed to bogging down the data mining process by filing reports on common transactions.

Based upon data that FinCEN provided to the Bank Secrecy Act Advisory Group's ("BSAAG") CTR Subcommittee, increasing the reporting threshold to $20,000 would decrease CTR filings by 57 percent and increasing the threshold to $30,000 would decrease filings by 74 percent. The impact of raising the dollar value is even more astonishing for community banks. An informal survey of ACB members conducted in June 2004 indicates that increasing the dollar amount to $20,000 would reduce community bank CTR filings by approximately 80 percent. With respect

[3] Bureau of Labor Statistics Inflation Calculator
www.data.bls.gov/cgi-bin/cpicalc

to community banks with commercial deposits, businesses of all sizes routinely conduct cash transactions over $10,000.

Emerging software technology is the latest fraud detection instrument used by banks to advance their compliance responsibilities. These systems are designed to identify transactions that are out of character for a typical banking profile or historical account activity, or transactions that are inconsistent with the due diligence the bank has collected on that customer. While a useful tool, automated detection is extremely expensive to purchase and maintain, and is generally not a viable option for main street community banks. According to an informal survey conducted by ACB's Regulation and Compliance Committee, account monitoring software for community banks often costs more than $30,000 to $50,000 (in some cases hundreds of thousands of dollars depending on the product) for the initial purchase and on average $5,000 a month thereafter for maintenance. Software detection is by no means a panacea, and does not replace the need for personnel to study the anomalies identified by the software to determine if the flagged activity warrants a SAR filing. The human aspect is particularly important with respect to SARs, but even in the case of CTRs, most community banks do not process enough CTRs each year to justify spending tens of thousands of dollars on software that automates the cash transaction monitoring and CTR filing process. As a result, these institutions must manually monitor and file CTRs, which is an increasingly time consuming responsibility.

TIME FOR ACTION

For the past several years, law enforcement has been working to develop improved data mining capabilities and new analytical tools to better use CTR data. It may be tempting for Congress to

refrain from proposing legislative remedies in the hopes that law enforcement is able to materially improve data retrieval and analysis. However, the wait and see approach ignores the compliance and economic burdens shouldered by all banks, and particularly community banks. It ignores the requirement that anti-money laundering reports provide "highly useful" information. It ignores the Money Laundering Suppression Act of 1994, which requires the number of CTR filings to be reduced by thirty percent. It also ignores the real-world realities of CTR filing. In the absence of meaningful regulatory relief, depository institutions will continue to file countless defensive SARs and CTRs on every cash transaction of $10,000 or more. While this approach will further bog down the investigation process, it is simpler and often more cost efficient than using the current exemption system.

CONCLUSION

Community bankers fully support the goals of the anti-money laundering laws, and we are prepared to do our part to fight crime and terrorism. ACB members are committed to ensuring our nation's security and the integrity of our financial system. However, we believe the existing statutory and regulatory regime is broken and needs to be repaired, and that the cumulative burden placed on community banks is out of proportion to the results that have been demonstrated to date. Increasingly, financial institutions believe that the federal government has little regard for the amount of time, personnel, and monetary resources that BSA compliance drains from an institution's ability to serve its community. What may seem like insignificant costs to law enforcement have very real business implications for community banks and their communities, and banks should not be expected to report transactions to law enforcement or conduct business in an environment that expects compliance at any cost. The time is now to

review the BSA compliance requirements to ensure that the burden shouldered by the nation's community banks is commensurate with the demonstrated benefit to law enforcement. Broad assurances that law enforcement is able to sift and mine the millions of SARs and CTRs that financial institutions file annually is not enough.

I wish to again express ACB's appreciation for your invitation to testify on this important matter, and I would be pleased to answer any questions you may have.

CHAIRMAN MELVIN L.WATT

SUBCOMMITTEE ON OVERSIGHT & INVESTIGATIONS, FINANCIAL SERVICES COMMITTEE

HEARING ON "SUSPICIOUS ACTIVITY AND CURRENCY TRANSACTION REPORTS: BALANCING LAW ENFORCEMENT UTILITY AND REGULATORY REQUIREMENTS"

THURSDAY, MAY 10, 2007

Questions for the Record

The Subcommittee appreciates your testimony in the above-entitled hearing on May 10. Below, please find follow up questions to which we request additional answers for the record. The Subcommittee would appreciate your written response on or before June 10.

William F. Baity, Deputy Director of the Financial Crimes Enforcement Network (FinCEN)

(1) Why was "BSA Direct" terminated in 2006? What, if anything, is replacing it?

Response

The Financial Crimes Enforcement Network (FinCEN) cancelled the BSA Direct Retrieval and Sharing Component (BSA Direct R&S) project in July 2006, and was the subject of a July 2006 GAO report entitled "Observations on the Financial Crimes Enforcement Network's (FinCEN's) BSA Direct Retrieval & Sharing Project." As discussed in our July 14, 2006 termination notification to Congress, the project repeatedly missed program milestones and performance objectives, and the performance of the BSA Direct R&S development system did not meet the needs of FinCEN's users. The level of effort and costs to complete BSA Direct R&S, address all remaining defects of the system, and operate and maintain the system, were estimated to be much greater than originally projected.

FinCEN has recently undertaken a comprehensive Modernization, Vision, & Strategy (MV&S) planning effort to formulate information technology (IT) capabilities to meet stakeholder needs. As result of the MV&S work, FinCEN has identified a number of options to meet its IT needs, which we will continue to explore and review with stakeholders. The MV&S process exemplifies an effective collaboration of BSA stakeholders.

(2) During your testimony, you referenced a "top-to-bottom" information technology review currently underway FinCEN. Please explain. What specific deliverables or

organizational changes do you expect as a result of this review? What reduction in burden to businesses required to complete SARs and CTRs do you anticipate from the review and why?

Response

In November 2006, FinCEN, in partnership with the Bureau's business leaders and stakeholders, initiated an effort to establish the organization's enterprise business transformation and IT modernization vision and strategy (MV&S). As part of this effort, the business and IT divisions came together to examine the collection, analysis, and use of the annual 16 million BSA filings, as well as how FinCEN serves its stakeholders. This initiative is based on a strong and effective collaboration of the internal and external stakeholders.

With regard to organizational changes, FinCEN's CIO introduced a new Information Technology organization (Technology Solutions and Services Division) and service delivery model on May 24, 2007 to support the MV&S effort. Strong emphasis is being placed on Customer Relationship, Safeguards and Assurance, and the IT Modernization initiative by establishing each of these as offices. FinCEN's senior IT management team has been augmented with experienced (averaging over 15 years each) program managers from industry and the federal government.

As part of the IT MV&S initiative, FinCEN identified new capabilities and performance targets to streamline reporting obligations of filers and increase feedback and notices to the filers. Under the auspices of the BSA Advisory Group (BSAAG), an IT subcommittee is being formed to further solicit industry input and response for new IT capabilities or initiatives on how to increase efficiency in completing and filing required reports. FinCEN is also exploring ways to use information technology to measure the impact of the data it collects on law enforcement efforts, which would help articulate the value of BSA filings to the financial community. In the meantime, FinCEN is actively working with the GAO on their CTR study.

(3) You testified that recent technological advances have improved the quality and efficiency of data that FinCEN shares with law enforcement and FinCEN is no longer merely a "library" of data. What obstacles remain to continual improvement of FinCEN's technological or analytical capabilities? What specific steps do you recommend to achieve the desired objective?

Response

Under an arrangement predating FinCEN's 1990 inception as an agency, the Internal Revenue Service (IRS) collects data reported under the BSA. The IRS Enterprise Computing Center (ECC) collects the reports, converts paper and magnetic tape submissions to electronic media, and corrects errors in submitted forms through correspondence with filers. The IRS-ECC also maintains the Web Currency and Banking

Retrieval System (Web CBRS), which is the primary BSA data query system and is available to federal, state, and local law enforcement and regulatory agencies.

However, the data analysis and management capabilities currently available via WebCBRS are limited for FinCEN's overall mission. For example, WebCBRS does not provide FinCEN with adequate data quality detection and reporting, advanced data analysis and pattern detection, and predictive analysis using geospatial data. In addition, numerous changes must be made to WebCBRS and other of FinCEN's IT systems to support the advancement of analytical abilities and to allow FinCEN to act in a more proactive capacity to its customers. Doing so will require increased collaboration between IRS-ECC and FinCEN.

FinCEN is undergoing a re-planning effort to address strategic, technical, and resource planning issues, as well as stakeholder analysis. In addition, we will continue our efforts with the Internal Revenue Service to implement WebCBRS as a means of meeting internal and customer needs for BSA data query.

(4) Testimony before the Subcommittee stressed the importance of FinCEN's proactive, analytic work. The Treasury Inspector General's 2006 Report indicated that by fiscal year 2005 such work accounted for 10% of FinCEN's total case load. What is the percentage of analytical work for this fiscal year? How is this percentage calculated? Is this number meeting expectations? Do you have any evidence that law enforcement has actually used your analysis?

Response

While both the Treasury Inspector General's report and FinCEN's testimony address the importance of FinCEN's proactive case work, it is important to note that FinCEN's strategic goal is to increase its overall production of "complex cases."[1] This includes support provided to all of FinCEN's customers, policy makers, and the regulatory community.

FinCEN's completed proactive cases have comprised 10-12 percent of all completed cases since 2005. In the first six months of fiscal year (FY) 2007, FinCEN completed 72 proactive cases, or 10 percent of the total completed cases (this is a straight percentage calculation).

During the same time period, FinCEN completed 55 complex cases (23 of these were proactive cases). This represents a weighted average of 20 percent of closed cases. Weighting is utilized to compensate for the additional analytical resources complex cases require.

[1] These products include synthesis of data from multiple sources, interpretation of findings and recommendations for action and/or policy. Examples are geographic threat assessments, analyses of money laundering/illicit financing methodologies, analytic support for major law enforcement investigations, and analysis of BSA compliance patterns.

These numbers do not meet our performance goals. Over the past few years, FinCEN has reduced the number of incoming non-complex cases from domestic law enforcement almost 75 percent by encouraging law enforcement to directly access the data through WebCBRS in an effort to focus on complex casework. These reductions have been offset by increases in foreign financial intelligence unit case requests, and FinCEN's increasing case work for requests from the Committee on Foreign Investment in the United States (CFIUS). Further impacting these calculations is that complex analytical products, by their very nature, require additional time and resources, resulting in fewer products and a smaller of percentage of total cases completed in a fiscal year.

Customer Feedback on Analytical Products

FinCEN conducts an annual Customer Satisfaction Survey for its case reports. The 2006 survey showed that more than two-thirds of respondents judged FinCEN's analytical information as useful, helpful in identifying new leads, providing new information, or helping to make better use of resources.

Since FinCEN redirected its analytical efforts toward specialized analysis of Bank Secrecy Act records in FY 05, FinCEN has produced proactive products for its law enforcement customers that are both strategic and tactical in nature.

Between FY 05 and FY 07, proactive tactical products were produced in two categories: (1) Terrorism financing referrals based on review and evaluation of Suspicious Activity Reports and, (2) investigative lead information that complemented or arose from strategic assessments of geographic areas, industries or issues. In both categories, FinCEN received feedback indicating positive follow-up to the tactical referrals. We have also received ad hoc feedback thanking FinCEN for individual reports that have been useful to law enforcement.

FinCEN continues to explore options for more directly assessing the law enforcement impact of its analytic products.

(5) According to the same Inspector General's report, in fiscal year 2005 FinCEN had not scheduled 28 of 66 required on-site inspections in accordance with its Gateway Inspection Policy and Procedure. The inspection of these sites, used by law enforcement to remotely access BSA data, is critical to determining whether such system use is proper and safeguarded. Is there still a backlog? How many inspections are scheduled for the coming fiscal year? How many have been completed in the present fiscal year?

Response

Currently there is no backlog of inspections. As of May 31, 2007, the Office of Liaison Service (OLS) had completed 14 of the 36 required FY 2007 inspections. There are 22 state, local and federal agencies inspections remaining for the year.

Of the 22 outstanding inspections, 14 have already been scheduled or conducted (but not reported/recorded), which leaves 8 federal agency inspections to be scheduled this year.

FinCEN hopes to complete these inspections by the end of the year. There are 69 required inspections currently projected for fiscal year 2008.

(6) Testimony before the Subcommittee indicated the desirability of improving communication between FinCEN and those organizations required to supply BSA data. What is FinCEN's plan to increase outreach, feedback and communication among the affected organizations?

Response

Successful implementation of the BSA requires a partnership with the financial institutions that file reports and maintain information pursuant to the BSA, as well as FinCEN's customers and other stakeholders in the data. Such a partnership enables FinCEN to communicate the impact of BSA data most valuable to our law enforcement, regulatory, and intelligence community customers, consistent with the purposes of the BSA, while minimizing burden and providing guidance to covered industries.

In 2007, FinCEN formed the Office of Outreach Resources to improve FinCEN's regulatory interface with the public, other customer and stakeholding agencies, and other parts of FinCEN. A key component of FinCEN's mission is communicating the need for, and impact of, FinCEN's Bank Secrecy Act (BSA) regulations, while also remaining open to the financial community on possible ways to reduce regulatory burden. To achieve this mission, the Office of Outreach Resources seeks to develop new regulatory outreach products and additional methods for their delivery, such as interactive CD-ROMs, video training modules on DVDs, and web-based video conferencing (webinars), as well as develop additional indicators of the impact of BSA regulations. The Office will also serve as liaison, receiving feedback from affected industries and reaching out on possible ways to minimize reporting burden. Producing additional regulatory outreach materials and BSA training products and utilizing cost effective means for their broader distribution will help strengthen the ability of FinCEN to reach the entities encompassed under the provisions of the Bank Secrecy Act.

FinCEN's outreach activities entail a variety of activities, including:

- Conducting liaison activities with the regulatory agencies that examine for BSA compliance to provide them with information concerning the impact of existing BSA requirements, including feedback that FinCEN has received from covered institutions. Also, where appropriate, encouraging possible changes/additions to existing requirements.
- Receiving feedback from affected industry on ways to reduce regulatory burden.
- Preparing and delivering training materials and programs to covered institutions.
- Operating a BSA "Regulatory Helpline" that serves as a resource for covered institutions with questions on BSA regulatory and compliance matters. Monitoring the questions received through the "Regulatory Helpline" to identify areas where FinCEN may need to clarify current regulations, rulings or guidance.

- Operating a BSA "Hotline" to assist covered institutions in reporting suspicious activity concerning terrorist financing in an expedited (i.e., time-critical) fashion.
- Coordinating initiatives of the Bank Secrecy Act Advisory Group (BSAAG) and its subcommittees, including preparation of the *SAR Activity Review* publication, which provides guidance and feedback to financial institutions.
- Analyze information gathered through various interactions with the BSA community, including covered institutions, state and federal regulatory agencies, law enforcement authorities, industry associations, Congress, and international bodies, to identify important concerns and trends with respect to BSA compliance.
- Conducting speaking engagements before constituencies interested in (and/or impacted by) the work of FinCEN, and developing presentations for delivery at speaking engagements, as appropriate.
- Developing and implementing processes to make the information and guidance pertaining to BSA requirements more readily accessible to covered institutions.
- Redesigning our public website to make information more accessible.

THE FINANCIAL SERVICES ROUNDTABLE

Impacting Policy. Impacting People.

1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

E-Mail info@fsround.org
www.fsround.org

June 11, 2007

Chairman Melvin L. Watt
House Financial Services Committee,
Subcommittee on Oversight & Investigations
Washington, DC 20510

Dear Mel:

On behalf of the member companies of the Financial Services Roundtable, I first want to thank you for your leadership on the recent hearing on "Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements." I hope my written responses to your questions are helpful in developing a record for the need to improve the effectiveness of our current Bank Secrecy Act (BSA) reporting system this calendar year.

1.) Please explain how your proposed "working group" consisting of regulators, FinCEN and financial institutions would work? How is your proposed group different from the existing Bank Secrecy Act Advisory Group (BSAAG)?

On question number one, we believe that this subcommittee should issue a formal bi-partisan letter convening a new "Bank Secrecy Act Working Group" charged with assessing the effectiveness of the current Bank Secrecy Act (BSA)/ Anti-Money Laundering (AML) reporting requirements and proposing appropriate reforms to Congress. This new working group would be comprised of federal banking regulators, FinCEN, law enforcement, and financial institutions. This group should be chaired by a neutral party, for example the Federal Reserve Board.

On the second part of question number one, the new BSA Working Group would be different from the existing BSAAG because of its specific core mission and goals to develop policy improvements to our current system. Moreover, Congress would require the group to set a time-table to analyze the effectiveness of the anti-money laundering and anti-terrorist financing requirements applicable to financial services firms and report these findings to Congress. Additionally, the group would have the following mandates:

- Assess and improve the effectiveness of the entire BSA reporting system;
- Study and compare BSA reporting system of other countries;
- Reduce the cost to consumers and compliance burden to financial institutions; and
- Increase the effectiveness of a new risk-based reporting system, focusing on targeted suspicious activity.

2.) Who are the members of BSAAG and how were they appointed?

Regarding question number two, the BSAAG is a task force established by Congress in 1994 for the purpose of giving the Treasury Department advice on strengthening anti-money laundering programs and simplifying currency reporting forms. The group is chaired by the Director of FinCEN and the Department of Treasury is a member ex officio. The 52 Member group consist of representatives of the following entities:
Federal Government: Federal Law Enforcement and Federal Regulatory Agencies;
State Government: State Regulatory Agencies (1), State Regulator Trade Groups (2);
Self-Regulatory Organizations: Securities Self-Regulatory Organizations (2) and Futures Self-Regulatory Organizations (1);
Industry Trade Groups: Banking (5), State Banking (2), International Banking (2), Credit Unions (1), Securities (1), Futures (1), Casinos (1), Money Service Businesses (2), Insurance (1), Dealers in Precious Metals, Stones, and Jewels (1), Mutual Funds (1), Investment Companies (1), and Gatekeepers (1);
Industry: Banking (6), Securities/Futures (3), and Money Service Business (1).

3.) What is the cost, on average, of the CTR software to your members? Is there a separate cost of SAR software? Is the software purchase a one-time cost or are there ongoing costs for software updates, patches, etc.?

With respect to question number three, we do not have any information on the CTR and SAR software related cost to our members. Moreover, while this is an interesting question, the "real cost" is the insidious outcome in denying consumers access to our banking system, management resources diverted from the core operation of the business (cost & time), increased risk adverse behavior of management, which is negatively impacting the economy, and a tax on law enforcement resources in trying to analyze almost 1 million SARS in 2005 and the 17 million CTRs filed annually.

Please let me know if you need further information.

Best regards,

Steve Bartlett
President and CEO

Responses of the Federal Bureau of Investigation Based Upon the May 10, 2007 Hearing Before the House Committee on Financial Services Subcommittee on Oversight and Investigations Regarding Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements

1. Mr. Hernandez, you testified that SARs and CTRs often initiate investigations. Please identify what percentage of investigations was initiated by SARs and CTRs in 2006 (or latest year available). Also please explain exactly how a SAR or CTR "initiates" an investigation? How are these reports used generally?

Response:

The FBI's case management system does not track how many Suspicious Activity Reports (SARs) or Currency Transaction Reports (CTRs) initiate investigations, but we are looking at ways to help capture indicators of the utility of these reports. In addition to initiating investigations, SARs and CTRs provide a wealth of financial intelligence that supports numerous FBI criminal, counterterrorism, and counterintelligence investigations. Both CTRs and SARs provide valuable information in identifying and evaluating assets and subject links. Historically, CTRs have been used less often than SARs as a case initiation tool, but more often than SARs as a source of financial intelligence to support ongoing investigations. The FBI has, though, recently begun proactively reviewing CTRs to identify potential frauds, focusing on CTRs related to the geographic areas and occupations most often linked to fraudulent activity. Transactions that fall well outside normal ranges are reviewed against other information, including SARs, commercial databases, and internal investigative data to determine whether a case should be opened. A number of case initiation leads have been developed using this method. In a review of the overlap between subjects under investigation and associated BSA reporting, the vast majority of the overlap (over 90%) is in CTR reporting.

Depository Institution SARs are regularly reviewed in the field by each field office's Field Intelligence Group (FIG). The FIGs were formed as a part of the FBI's evolution into a more intelligence-driven agency. Generally, SARs are routed to the appropriate FIG for review, based on where the suspicious activity occurred. The FIGs analyze and disseminate the information to the appropriate substantive supervisor for possible case initiation or to support ongoing investigations. SARs are also reviewed to monitor new and ongoing trends, such as in mortgage fraud schemes and changes in the black market peso exchange.

Information on these trends is distributed to the financial industry through the Financial Crimes Enforcement Network's (FinCEN) Suspicious Activity Reviews.

The FBI accesses SARs, CTRs, and the other Bank Secrecy Act (BSA) reports both through direct access to FinCEN's web-based Currency and Banking Retrieval System (WebCBRS) and through regular downloads of the data into the FBI's Investigative Data Warehouse (IDW). The question to be answered with the research will dictate the system to be used for accessing the data. The availability of this information in IDW allows us to use the BSA data in ways not previously possible. For example, the FBI has recently completed development of a proactive SAR link analysis tool to identify criminal networks. Various search criteria such as the violation dollar amount, geographic area, and violation type are used to identify links between individuals and/or entities reported in SARs. Resulting "clusters" are then further analyzed to assess the need for follow-up investigation. This tool is very new and in only limited use in FBI field offices. While we cannot yet determine how successful this tool will be in developing the information needed to initiate cases, initial feedback from the field is very positive and we believe this tool will enhance the FBI's investigative capabilities.

Other tools are further increasing the value of the SARs. For example, one tool alerts a field office when a SAR is filed on a subject currently under investigation by that office, even when the SAR is assigned to another field office based on the location of the suspicious activity. Another tool allows field offices to search the various SARs filed in their territories for specific violations. Those identified in these SARs can then be checked through IDW to obtain more complete pictures of their activities.

2. *See* Brian Maass, *FBI didn't check bank's suspicion about checks*, ROCKY MOUNTAIN NEWS, May 10, 2007 (attached). How did this case fall through the cracks? Is the failure to follow up on the SAR in this case a persistent problem within the FBI? What is the FBI or Department of Justice policy in place to ensure this does not happen regularly and that it does not happen again.

Response:

The FBI, which is one of a number of law enforcement agencies using SARs, uses these reports as a basis for potential case initiation and to support ongoing investigations. Although the FBI does refer some SARs to other agencies, this is not an FBI responsibility. There are approximately 80 multi-agency SAR Review Teams around the country headed by each team's local U.S. Attorney's Office, and the FBI participates on many of these teams. These teams

review SARs to determine the need for follow-up investigations and the most appropriate agencies to conduct those investigations. In the case referenced in the question, the SAR was reviewed by the Denver SAR Review Team and selected for follow-up investigation. It appears from press accounts that the Colorado Department of Revenue came upon other information leading them to refer the matter to state law enforcement authorities, who also decided to investigate the matter. This SAR did not "fall through the cracks" but, instead, it appears that investigative activity was initiated by different agencies on parallel tracks following slightly different time lines.

3. The Treasury Inspector General's report on FinCEN for the year 2005 states that there has been little progress in improving the quality of SARS data, and consequently their value to law enforcement is diminished. How can the quality of SARs be improved?

Response:

There are different ways to define SAR data quality. One involves the quality of the SAR's description of the activity it is reporting and another involves the quality of the information filling the various data fields of the SAR. Overall, we believe the banks are doing an excellent job of providing well thought out and detailed narrative descriptions of the suspicious activity. While some SARs are not as complete as we would like, the quality is very good overall. FinCEN has published guidance to the banks to assist in improving SAR content, and we are conducting increased outreach to help the financial community understand how we use the information and the benefits we are deriving from it. The FBI believes this dialogue assists the banks in providing more meaningful SAR reporting.
As to the quality of the information in the SAR's fields, we do continue to find problems with the data entry on SARs, including recurring problems with missing or erroneous entries in the date field (i.e., 13/59/9999), amount field, and bank information field (such as erroneous or incomplete names, addresses, and account numbers). When using electronic tools to review and analyze SARs, we have to devote additional resources to "cleanse" the data in order to ensure a more meaningful and complete analysis. For example, different SAR preparers within the same bank may enter their bank's name in different ways, such as "ABC BANK" versus "ABC BK," or "XYZ CREDIT UNION" versus "XYZ CU" or "XYZ FCU". Without cleansing or normalizing the data first, the software will interpret these variations as representing different entities, making analysis far more difficult.

As mentioned above, the FBI developed a proactive SAR link analysis tool, but the tool could not be applied until we completed approximately nine months of extensive data cleansing and developed data cleansing rules to address some of these issues in new SARs. For example, the initial set of almost three

million SARs contained 547,000 different bank branch names. After cleansing the names, these 547,000 entities collapsed down to 160,000 different bank branches. Although rules can be written for bank name and address fields, these rules cannot correct missing or erroneous data.

Based on our experience working with large BSA data sets, it is clear that electronic filing of all SARs and other BSA reports is more useful for analysis than other filing methods. Electronic filing should include appropriate data input controls to facilitate the use of electronic analysis tools employed by the FBI and other law enforcement agencies. These controls could include such things as ensuring that certain mandatory fields are completed and that dates entered are plausible (meaning, for example, the month field would only accept values of 1 through 12). Fields such as the bank and branch name should be automatically populated so this information is entered in the same manner on every SAR filed by a particular bank. The U.S. Postal standard should be mandated for all address fields.

4. The Department of Justice, in a letter dated April, 6, 2006, appended to GAO Report 06-386, "Bank Secrecy Act-Opportunities Exist for FinCEN and the Banking Regulators to Further Strengthen the Framework for Consistent BSA Oversight", suggests that the examiner forms and SARS forms' use of a "checklist" may not be as effective in detecting criminal activity as other methodologies. Does the Department of Justice or FBI have suggestions for an improved SARS form, including the increased capture of identifying data? Does it confer with other law enforcement agencies, the DEA for example, in an effort to improve such forms?

Response:

When the SAR and other BSA forms undergo revision, consideration must be given to the fact that electronic tools largely drive the analytical process. As mentioned above, the use of electronic SAR filing would greatly enhance its value and utility to law enforcement. In addition to the identifying data currently being captured, email addresses and telephone numbers (to the extent known by the bank) would be very beneficial as well, because valuable link analysis can be conducted using this information. The structure of the name fields should be revised to allow analytical software to better "read" whether the suspect/transactor/owner is an individual or a business. (The importance of this capability is illustrated in the current debate on CTR reporting, which has recognized the importance of being able to reliably distinguish between individuals and businesses.)

The FBI does confer with other law enforcement agencies on improvements to BSA forms; this is typically done through each agency's liaison

to FinCEN. During the latest revision of the bank SAR form, the FBI and other law enforcement agencies had the opportunity to make suggestions. These suggestions were reviewed by FinCEN in consultation with the regulators who ultimately decided which suggestions would be accepted.

Rocky Mountain News

To print this page, select **File** then **Print** from your browser

URL: http://www.rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_5529497,00.html

FBI didn't check bank's suspicion about checks

By CBS 4 Reporter Brian Maass, Special to the Rocky
May 10, 2007

A downtown bank alerted federal authorities late last year that it had suspicions about Hysear Don Randell, but the Denver FBI office failed to follow up on that red flag and didn't pass along the information.

Hysear, 40, is the hip-hop entrepreneur suspected of teaming with his girlfriend in a scheme to steal $10 million from the Colorado Department of Revenue, where she worked.

Michelle Cawthra, a supervisor in the taxpayer services division, was arrested April 28 and accused of funneling the taxpayer money from state accounts into bank accounts controlled by Randell.

Department administrators learned of the theft last month.

But UMB Bank raised concerns about Hysear five months earlier, sources told CBS 4.

The bank at 1670 Broadway filed a "suspicious activity report" on Dec. 29, detailing at least five pages of information on how numerous checks from the state of Colorado had been deposited into Randell's accounts.

Sources said one of the state checks deposited into Randell's account that raised a red flag was close to $200,000 and another check was for more than $200,000.

Rene VonderHaar, a spokeswoman for the FBI in Denver, confirmed the local office received UMB's suspicious activity report in January, but did not investigate it.

"It fell through the net," she said.

VonderHaar said the Denver office receives about 800 suspicious activity reports each month from local banks, and only about 100 receive additional scrutiny. Even fewer are fully investigated, she said.

"We have parameters to look at a case. Since it did not have a connection to terrorism or a cash loss for a bank, it did not hit our priority level."

Randell and Cawthra are both being held on $10 million bail each.

Contact Brian Maass at bmaass@cbs.com

Copyright 2007, Rocky Mountain News. All Rights Reserved.

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

Response to Questions for the Record

On Behalf of the
American Bankers Association
Before the
Subcommittee on Oversight and Investigations
Committee on Financial Services
United States House of Representatives

Hearing on Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements

Thursday, May 10, 2007

The American Bankers Association (ABA) is pleased to have the opportunity to provide you with the following responses to questions for the record delivered on May 29, 2007 to Megan D. Hodge, Director of Anti-Money Laundering (RBC Centura Bank) who testified on behalf of ABA in the hearing on "Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements," conducted May 10, 2007. We will briefly provide you with information pertaining to recommendations proposed by the ABA in its written testimony to address better tracking and reporting of cases resulting from the filing of a SAR by both the Financial Crimes Enforcement Network (FinCEN) and the Department of Justice (DOJ), industry cost burdens to ensure BSA compliance, and customer privacy concerns.

You requested responses to the following questions recited below in boldface.

On page 7 of your written testimony, you propose that FinCEN and DOJ institute a "tracking system" of SAR outcomes to reflect law enforcement results. How would this work? Explain the potential benefits to the financial industry from such a tracking system.

ABA has in mind a tracking system similar to the mechanism currently being used by FinCEN to track and report law enforcement's utilization and success of the USA PATRIOT Act's §314(a) reporting requirements. Periodic fact sheets are issued by FinCEN describing the success of the feedback process through detailed numbers reflecting the various stages of the process, including new accounts and transactions identified, grand jury subpoenas, search warrants, arrests, indictments, convictions and total dollar amount located by law enforcement. We understand that this tracking mechanism is entirely controlled by FinCEN and the law enforcement

agencies that utilize the 314(a) process. Banks have no reporting or input obligation for the results tracking mechanism.

Similarly, ABA envisions a results tracking system for SARs that would be the obligation of FinCEN and the law enforcement and regulator community that utilize SAR data. Banks would have no obligation for generating any additional reporting information. Instead, each agency that accesses SAR data would be required to track how such data was used by the agency in pursuing law enforcement remedies and to report to FinCEN through a program of their devising. Implementation of such a program would provide law enforcement, regulatory agencies, Congress and the private sector with information on the utilization of, and results derived from, the reports being filed. Although FinCEN currently issues overall statistical information about reporting trends, they do not provide a breakdown that follows how industry responsiveness to its SAR requirements translates, on a report-by-report basis or even a case-by-case basis, into concrete law enforcement results. After all, the purpose of the SAR reporting process is not to generate descriptive crime statistics, but rather to provide real leads for law enforcement to catch criminals and terrorists. Such results are not being systematically measured and should be. Only through such measurement and public feedback can banks, policy-makers and others evaluate the real benefit in law enforcement results that flows from the substantial burden banks and other financial institutions undertake by virtue of the SAR process.

What is the average cost of annual BSA compliance to your members? If possible, please differentiate between the cost of automated software and the cost of training and man-hours spent reviewing and preparing SARs.

The issue of cost and resource allocation is a consistent challenge for financial institutions. There has not been a comprehensive formal industry-wide study by ABA of Bank Secrecy Act (BSA) costs as the process and methodology to achieve compliance vary dramatically from institution to institution. There are many factors to take into consideration when discussing cost and budget allocation for anti-money laundering (AML) and counter-terrorist financing (CTF) compliance, including staff, automation tools, training, independent audit, reporting requirements, and documentation retention. Furthermore, the cost of compliance varies based on the size of the institutions, the degree of centralization of processes and the level of automation. Finally, the breadth of SAR filing embraces a broad range of illegal activity including fraud, computer intrusion, identity theft and other scams that implicate another set of widely varying bank regulatory and control costs.

ABA has had occasion to discuss this topic with various members and based on a small sample of institutions that were able to provide some budget information, we estimate that dedicated BSA/AML/OFAC compliance program costs for the banking industry approaches $2 billion annually. This is based on budgets for dedicated BSA/AML/OFAC compliance units including dedicated staff salaries and related technology costs (about $500 million of the estimate) plus the approximate value of time spent by bank staff to receive BSA/AML training (about $200 million.)

Fraud investigative or loss mitigation activity that may lead to SAR filing is <u>not</u> captured by this estimate. In addition, this dedicated BSA compliance program estimate does <u>not</u> include the time spent by tellers or other business line staff to

conduct customer due diligence, monitor transactions or report suspicious or other activity vis-à-vis SARs or CTRs.

Are there documented privacy concerns among customers of RBC Centura or other members of the ABA resulting from the filing of SARs and CTRs? Can you give an estimate of how many customers RBC Centura or ABA members as a whole lost in 2006 as a result of privacy complaints regarding SARs and CTRs?

Privacy and information security concerns are of utmost importance and in the forefront for financial institutions reporting on suspicious activity. There are no case studies or statistical information pertaining to specific situations where customers have voiced concern over the privacy and security of their non-public personal information. Recently, the ABA has been informed of an Internal Revenue Service (IRS) - Criminal Investigations Division (CID) investigative process, as described in the written testimony that raises concerns of jeopardizing the safe harbor provisions of SARs. This "Knock and Talk" program has been experienced by several ABA members; but to date, RBC Centura has not had a customer approach them in a way that identifies them as having such an experience. Nevertheless, since our testimony, other banks have described to us similar incidents where they have been confronted by customers who have received a visit or a letter from the IRS. These customers have expressed varying degrees of concern or outrage about the bank's handling of their confidential financial affairs. We understand from some banking regulators that they have seen copies of letters sent to bank customers by both IRS and Assistant United States Attorneys. ABA has received a partially redacted copy of one such letter. We provide it as an attachment to this response.

Unfortunately there are no publicly available statistics to track the number of letters sent or verbal communications conducted between bank customers and the IRS or Assistant United States Attorney offices. In May, ABA conducted an open survey of visitors to its compliance web page that asked the following question, "Have any of your customers reported to you that they received a letter or a visit from an IRS agent alleging they were engaged in structuring?" We found that from the 111 responses received, 5.4% responded in the affirmative. This anonymous informal survey is the only statistical information obtained by the ABA of the prevalence of this concern. Neither RBC Centura, nor ABA has any estimate about the amount of lost business incurred as a result of these types of incidents.

ABA stands by its testimony and believes that this approach by IRS and other law enforcement agents should stop.

The ABA thanks the Subcommittee for this opportunity to provide additional clarification and information pertaining to these issues. Should the Subcommittee have further questions, please feel free to contact Richard Riese, Director of ABA's Center for Regulatory Compliance, (202) 663-5051, rriese@aba.com .

Dated: June 8, 2007

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CRIMINAL INVESTIGATION

Dear Mr.

A Federal law known as the Bank Secrecy Act (Title 31, United States Code, Section 5311, et. seq.) requires banks and other financial institutions to report large currency transactions to the Financial Crimes Enforcement Network. This reporting is done on FinCEN Form 104 (Currency Transaction Report) and is required for all cash transactions over $10,000.

The same law prohibits individuals from causing a financial institution to fail to file such a report or to file a false report. The law specifically prohibits individuals from attempting to structure a currency transaction in any manner designed to avoid the filing of the report and provides both criminal and civil penalties for such acts.

I have reason to believe that you, or others on your behalf, may have conducted financial transactions that appear to be in violation of the Bank Secrecy Act.

Additional information concerning Currency Transaction Reporting Requirements and Forms 8300 can be found on the Financial Crimes Enforcement Network (FinCEN) website, www.fincen.gov. If you have any questions, please feel free to call Special Agent

Sincerely,

Attachment 1 to ABA Response to
Questions for the Record
Subcommittee on Oversight and Investigations
House Financial Services Committee
May 10, 2007

Submitted June 8, 2007

Question

You testified that it is not "practical" for small, community banks to take advantage of the exemptions for CTRs. Briefly explain why this is so. Is the primary impediment the BSA/AML Examination Manual, resource constraints, fear of regulatory action for incorrect use of exemptions or something else?

Answer

FinCEN had the best interests of financial institutions in mind when it developed the CTR exemption, and it should be credited for making an effort to mitigate some of the BSA compliance burdens. However, filing a CTR on all reportable transactions is the best way for Bay-Vanguard to manage compliance costs and regulatory risk.

While the exemption may be a helpful tool for large institutions with economies of scale, it is not cost effective for community banks like Bay-Vanguard to use the exemption system. Advances in technology and computer software have made it more cost efficient to file a CTR on each reportable transaction than it is to use the CTR exemptions. By contrast, the exemption regulations are very complex, labor intensive, and costly to use. We lack the time and resources to:

- Interpret and apply the regulations to determine whether a customer is eligible for the exemption.
- Document the decision to exempt a customer.
- Monitor a customer's continued eligibility for the exemption.
- File forms with the Department of the Treasury every two years to renew a customer's designation of exemption.

Our decision not to use the exemption system is more than a cost issue. Filing on all reportable transactions also helps Bay-Vanguard to reduce its compliance and regulatory risk. While the exemption procedure was developed with the best intentions, it still lacks a safe harbor. As a result, an institution that applies the exemption rules incorrectly could be subject to regulatory action. In this era of heightened regulatory scrutiny of BSA compliance, it is less risky for small banks to simply automate the process and file a CTR on every transaction that triggers a reporting requirement.

O

California Credit Union League
Serving Credit Unions in California and Nevada

May 10, 2007

The Honorable Gary Miller
Ranking Minority Member
Subcommittee on Oversight and Investigations
Committee on Financial Services
House of Representatives
Washington, DC 20515

Dear Ranking Member Miller:

On behalf of the California and Nevada Credit Union Leagues, I appreciate the opportunity to submit a letter for the record regarding the Subcommittee's Hearing on "Suspicious Activity and Currency Transaction Reports: Balancing Law Enforcement Utility and Regulatory Requirements" held on May 10, 2007. The California and Nevada Credit Union Leagues are the largest state trade associations for credit unions in the United States, representing the interests of more than 500 credit unions and their 10 million members. Today, however, we are writing regarding the compliance burden shared by all the nation's 8,536 credit unions due to the requirements of Suspicious Activity and Currency Transaction Reports.

All credit unions—regardless of size, field of membership, or charter type—must comply with the Bank Secrecy Act (BSA) and the Financial Crimes Enforcement Network's (FinCEN) implementing regulations, including the filing of Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs). And, as have other financial institutions, credit unions have been supportive of lawmakers' and regulators' recent stepped-up enforcement efforts regarding BSA and the filing of SARs and CTRs. For example, FinCEN's SAR Activity Review reports covering the period from December 2004 through June 2006 show that SAR filings made by credit unions as a percentage of all SARs filed by financial institutions have more than doubled. Through efforts such as these, credit unions are actively engaged in assisting law enforcement in detecting and deterring terrorism, money laundering, and other unlawful activity.

Proportionately, however, these efforts represent a greater burden on credit unions than other financial institutions, as the average credit union in the U.S.—at $85 million in assets—is far smaller than the average bank. By way of comparison, at $133 million in assets, the smaller of the two banks represented at today's hearing is larger than 88 percent of all credit unions in the U.S. In California and Nevada, 418 of the states' 565 credit unions are smaller than $133 million in assets.

Over three-fourths of U.S. credit unions have fewer than 20 full-time equivalent (FTE) employees, while two-thirds of U.S. credit unions have fewer than 10 FTEs. In California and Nevada, over 60 percent of credit unions have fewer than 20 FTEs, while over half have fewer than 10 FTEs. For such small credit union staffs, the time and resources needed to track,

9500 Cleveland Avenue, Suite 200 • Rancho Cucamonga, CA 91730-5929 • 909.980.8890
P.O. Box 3000 • Rancho Cucamonga, CA 91729-3000 • 800.472.1702 • www.ccul.org

evaluate, report, and follow up on transactions that currently trigger SAR and CTR filings is an enormous drain on their efforts to service members.

For that reason, we enthusiastically support recent efforts by FinCEN to revise the SAR form to help reduce the number of duplicate reports filed for a single suspicious transaction. In addition, we wholeheartedly endorse H.R. 323, the Seasoned Customer CTR Exemption, which would grant an exemption from CTR requirements for credit union members and bank customers with whom there is a regular and continuing relationship. FinCEN estimates in the CTR instructions that the average time needed to compete one CTR form is 19 minutes. H.R. 323 has the potential to greatly ease the compliance burden for all financial institution staff.

In closing, the California and Nevada Credit Union Leagues would like to thank the Subcommittee for the opportunity to provide additional information for the record about how America's credit unions contribute to—and are impacted by—SAR and CTR reporting. We applaud the Subcommittee's efforts to strike an effective balance between the needs of law enforcement and sensible regulation, and look forward to assisting you and your colleagues in doing so.

Sincerely,

Bill Cheney
President/CEO
California and Nevada Credit Union Leagues

9500 Cleveland Avenue, Suite 200 • Rancho Cucamonga, CA 91730-5929 • 909.980.8890
P.O. Box 3000 • Rancho Cucamonga, CA 91729-3000 • 800.472.1702 • www.ccul.org

O