STATEMENT OF WILLIAM J. FOX, DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK
UNITED STATES DEPARTMENT OF THE TREASURY

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

MAY 26, 2005

Chairman Kelly, Congressman Gutierrez, and distinguished members of the Committee, I appreciate the opportunity to appear before you to discuss the Financial Crimes Enforcement Network's administration and implementation of the Bank Secrecy Act, as amended. We thank you for the support and policy guidance you and the members of this Committee have offered to us on these issues. We are more certain than ever that the efforts undertaken by both the government and the financial industry under the Bank Secrecy Act are critical components to our country's ability to utilize financial information to combat terrorism, terrorist financing, money laundering and other financial crime. In addition, the systems and programs that are mandated by the Bank Secrecy Act that have been developed and are continuing to be refined make our financial system safer and more transparent.

Much has transpired since I last had the honor of testifying before this Committee. Significantly, Treasury's Office of Terrorism and Financial Intelligence has been stood-up and staffed. This has been a very positive development for the Financial Crimes Enforcement Network. Thanks to the leadership of Under Secretary Stuart Levey and Assistant Secretary Juan Zarate, Treasury, its bureaus, and offices that work on issues relating to financial intelligence, financial crime and sanctions are not only better coordinated, but also are developing previously uncovered synergies utilizing Treasury's unique tools, capabilities and financial perspective. This work has helped address the significant strategic threats of our time such as terrorism, drug trafficking, the proliferation of weapons of mass destruction and addressing rogue regimes.

In June of last year, because of the direct support of the Congress – especially Chairman Oxley and you, Madam Chairwoman – the Financial Crimes Enforcement Network awarded a contract to EDS to build the heart of the system that we are calling BSA Direct. This system, when complete, will revolutionize the way information under the Bank Secrecy Act is collected, housed, analyzed, disseminated and exploited. EDS is building the data warehouse that will eventually connect to our already existing e-filing system and other systems that control the access and dissemination of Bank Secrecy Act data. Scheduled for completion in October, BSA Direct's data warehouse will provide law enforcement, regulatory and other government officials, who are authorized to access Bank Secrecy Act data, a secure, modern, web-based data environment with robust and flexible search and data mining tools. BSA Direct, when fully complete, will for the first time enable the Financial Crimes Enforcement Network to discharge its most important responsibility – to collect, house, analyze and properly disseminate information collected under the Bank Secrecy Act – in an effective manner.

As the administrator of the Bank Secrecy Act, there is no duty I view as more critical than the effective collection, management, and dissemination of the highly sensitive and confidential information collected under that Act. If the Financial Crimes Enforcement Network does nothing else, we must ensure that we properly perform these functions. This is our core responsibility. There are a number of significant issues surrounding the collection and use of Bank Secrecy Act reports, and I welcome this opportunity to discuss those issues with you. A recent report issued by the General Accounting Office identified disturbing security problems related to the systems that currently handle Bank Secrecy Act data. The GAO reported recently that security problems in those systems exposed Bank Secrecy Act data to potential unauthorized access by users in the facility that houses the systems. We are profoundly concerned about the issues the GAO identified. The Financial Crimes Enforcement Network is the delegated steward of this data and is ultimately responsible for its security. We will move very quickly to take all appropriate steps to ensure this data is protected.

Since last year, we have focused great attention on issues relating to our responsibilities for administering and implementing the Bank Secrecy Act. Under the leadership of Associate Director William Langford, we have changed the way we interact with the regulators who have the responsibility of examining financial institutions for compliance with Bank Secrecy Act requirements, resulting in better coordination and communication with the industry. Because these issues go to the heart of the hearing today, I will discuss them in greater detail later.

We are changing the way we analyze information at the Financial Crimes Enforcement Network. We are moving away from the notion of "FinCEN as a library," with FinCEN analysts acting as librarians assisting customers with efforts to retrieve and understand Bank Secrecy Act data. Our new analytical paradigm requires higher-level research and analysis utilizing all sources of information to understand and explain the cutting-edge problems relating to money laundering and illicit finance, including terrorist

financing. Our goal is nothing short of being as good as, if not better than, any other analytic unit focused on financial issues in the world.

We have reengaged internationally, working with our colleagues in other financial intelligence units in ways that go far beyond simple information sharing. We are utilizing the powerful tools granted to us in Section 311 of the USA PATRIOT Act to safeguard the U.S. financial system from jurisdictions and institutions that are of primary money laundering concern. These actions have very serious and real effect, bringing change where change is needed, and at the same time letting the world know that we will not tolerate jurisdictions or institutions with little transparency or lax controls.

Finally, we are changing the way we interact with our law enforcement customers. I am very happy to appear here today with my good friend and colleague Mike Morehart, who is Chief of the Terrorist Financing Operations Section in the Counterterrorism Division of the Federal Bureau of Investigation. Special Agent Morehart's office is working tirelessly to keep our country safe from terrorists. Everyday, the men and women in the Terrorist Financing Operations Section quietly, and often thanklessly, accomplish their mission to identify, locate, disrupt, deter and capture terrorists attempting to harm the citizens of our country. They do their job utilizing some of the most valuable information available to the government – financial information – in the process. I know, as I have seen them at work, and I am aware of the fruits of their labor. As you will learn today, the Financial Crimes Enforcement Network has entered into a very deep partnership with the FBI that is allowing Mr. Morehart's office and other components of the Bureau to exploit the information collected under the Bank Secrecy Act in a much more meaningful and relevant way. We now provide wholesale access to the Bank Secrecy Act data to the FBI, which incorporates the Bank Secrecy Act data in their own Investigative Data Warehouse, where FBI users can query and analyze Bank Secrecy Act data in context with other information collected by the FBI. As we build BSA Direct, the Bureau will provide us in an automated way, the audit and other information necessary for us to discharge our responsibilities relating to the use of the data and to perform our networking function. The early results of the FBI's use of the data have been astounding, and I am sure Special Agent Morehart will share some of these statistics with you today. I am certain that this partnership makes us all safer. I am also certain that this partnership enables the Financial Crimes Enforcement Network to better achieve its mission to safeguard the financial system from the abuse of financial crime.

Everyone in this room knows that September 11th changed the world. What we may not have realized on that bright morning nearly four years ago, we now know for certain: September 11th revealed a new reality – a new paradigm. All the way back to Rome, the paradigm has been that governments can protect their citizens with military might or walls. We learned on September 11th that threats to our nation can no longer solely be met with military might or walls. Our enemies can come from within. They can be neighbors; people shopping at the same grocery store; getting gas from the same stations; using the same ATMs; or, taking the same flight. This new threat demands a

different way of looking at things, a different way of protecting our citizenry. No longer can any of us be passive about the defense of our country. The government cannot do it alone. What we know about this new reality is that ***information*** is a key to the security of a nation, and information is what the Bank Secrecy Act is all about.

I believe that through the USA PATRIOT Act, the Congress recognized this new reality. You broke down walls that prevented the sharing of information between law enforcement and the intelligence community. Most significantly to the issues being addressed today, you provided us tools to better acquire and share information both between the government and financial institutions, and between financial institutions themselves. These tools highlight a couple of important truths. First, that information sharing really is necessary and important to the national security. Secondly, these tools demonstrate the recognition that financial information, in particular, is highly reliable and valuable to identifying, locating and disrupting terrorist networks that mean to do us harm.

That is why this hearing is so timely and important. Your hearing today has been titled: "The First Line of Defense: The Role of Financial Institutions in Detecting Financial Crimes." Since the beginning of the year, I have traveled across the country and have spoken with bankers, broker dealers, money services businesses, and other financial institutions. These financial institutions have expressed candid concern about how the Bank Secrecy Act is being implemented. I am certain many of you have heard from constituent financial institutions expressing the same concern. Today, we will try to outline for the Committee those concerns, and what we are attempting to do to address them. From my perspective, nothing is more important, simply because I believe that financial institutions are the first line of defense to the security of our financial system. Consequently, we must proceed with the financial institutions in a collaborative way. It must make the partnership envisioned by the USA PATRIOT Act real, if we are to truly achieve our goals.

The goals of the Bank Secrecy Act are simple: (1) safeguarding the financial industry from the threats posed by money laundering and illicit finance by ensuring the financial industry – the first line of defense – has the systems, procedures and programs in place to protect the institution and, therefore, the system from these threats; and, (2) ensuring a system of recordkeeping and reporting that provides the government with the right information - relevant, robust and actionable information that will be highly useful in efforts to prevent, deter, investigate and prosecute financial crime. It is my view that the best way to achieve these goals is to work in a closer, more collaborative way with the financial industry. This regime demands a partnership and an on-going dialogue between the government and the financial industry if it is ever going to realize its true potential. It is why, for example, we are working so hard to implement Section 314(a) of the USA PATRIOT Act in a much deeper way, which will result in a sensitive, yet systemic, two- way dialogue with the financial industry. This dialogue will not only help make our country safer, but also it will educate our financial industry about the risks associated with its business lines and its customers. Knowing more about that risk will

make our financial system safer and more transparent. I am convinced that the financial industry is committed to this partnership and dialogue. Our goal is to do all we can to ensure that the government lives up to its side of the bargain.

As you are aware, while the Financial Crimes Enforcement Network is responsible for ensuring compliance with the Bank Secrecy Act regulatory regime, we do not examine financial institutions for compliance. Instead, we have delegated examination responsibilities to other federal regulators. Even in the absence of examiners, we have a critical role in supporting the examination regime created through our delegations. Following the events of last summer, with the support of Congress generally and this Committee in particular, we made dramatic changes within the Financial Crimes Enforcement Network to enhance our ability to support the examination function and better ensure consistency. We created an entirely new Office of Compliance, within our Regulatory Division, devoted exclusively to supporting and coordinating the examination function being carried out by other agencies. To ensure better utilization of our data, we devoted a significant portion of our analytical resources to supporting our regulatory functions. Within this broad framework, our role in the examination process begins with the issuance of regulations, continues with the provision of prompt Bank Secrecy Act interpretive guidance to regulators, policy makers and the financial services industry, and culminates with ensuring the consistent application of the Bank Secrecy Act regulations across industry lines. We promote Bank Secrecy Act compliance by all financial institutions through communication, training, education and outreach. We support the examination functions performed by the other agencies by providing them access to information filed by financial institutions in suspicious activity reports, currency transaction reports, and other Bank Secrecy Act reports. We also facilitate cooperation and the sharing of information among the various financial institution regulators to enhance the effectiveness of Bank Secrecy Act examination and, ultimately, industry compliance.

As my colleagues in the regulatory agencies and I are well aware, financial industry members across the spectrum are genuinely concerned about the heightened levels of scrutiny being placed upon their institutions. Unfortunately, we continue to see some institutions with very basic compliance failures that have a significant impact, while at the same time, we see institutions across the spectrum working harder than ever to ensure compliance with this regulatory regime. These institutions perceive a significant regulatory and reputation risk being placed upon their institutions by examiners, prosecutors and the press. This perception is not unfounded. Institutions are trying hard to determine what it takes to comply with the Bank Secrecy Act regulatory regime in this time of heightened scrutiny.

Financial institutions have stated loudly and clearly that they are concerned about the regulatory and reputation risk associated with their compliance with the Bank Secrecy Act. There is a perception held by institutions that their examiners have changed the rules of the game. There is also a palpable fear amongst institutions that a Bank Secrecy Act failure today will subject the institution to scrutiny by the Department of Justice and

a potential criminal action. We believe these concerns have had two principal consequences in the past year.

First, we believe many institutions are now filing some of their suspicious activity reports "defensively." In other words, institutions are filing on activity that does not meet the threshold set forth for filing by the regulations and guidance issued about when to file a report. Secondly, we believe that concern about the regulatory and reputation risk associated with the Bank Secrecy Act has led many financial institutions to reassess the risks associated with some of their customer base. This reassessment of risk is not a bad thing; in fact, many in the financial industry have told us that the heightened emphasis on Bank Secrecy Act compliance has caused their institutions to "know" their customers better. However, the ongoing reassessment of risk has also led many institutions to conclude that certain customers pose too much risk for the institution to continue to maintain an account relationship. These institutions have begun to terminate their so-called "risky" account relationships, the money services businesses sector, embassy banking and certain correspondent banking relationships are all industry sectors that have suffered the widespread termination of banking services. Unfortunately, we are concerned that often decisions to terminate account relationships may be based on a misunderstanding of the applicable Bank Secrecy Act requirements, or on a misperception of the level of risk posed.

With respect to the "defensive filing" of suspicious activity reports, at risk is the quality of the information reported. These reports not only provide law enforcement, regulatory agencies and other authorized officials leads indicative of illicit activity, but also provide a fertile source for identifying trends and patterns of illicit activity, as well as compliance-related deficiencies.

We estimate that if current filing trends continue, the total number of suspicious activity reports filed this year will far surpass about 700,000, an increase of more than thirty-seven percent over last year. Preliminary analysis of some of these filings supports the fact that some of this increase is attributed to defensive filing. While the volume of filings alone may not necessarily reveal a problem, it fuels our concern that financial institutions are increasingly becoming convinced that the key to avoiding regulatory and criminal scrutiny is to file more reports, regardless of whether the conduct or transaction identified is indeed suspicious. Such defensive filing results in our database becoming populated with reports that should not have been filed, diluting the value of the information in the database and implicating privacy concerns. Financial institutions from the smallest community banks and credit unions to the largest money center banks are telling us that they would rather file than face potential criticism after the fact.

If these trends continue, consumers of the data – law enforcement, regulatory agencies and intelligence agencies – will suffer. While the most sophisticated analytical tools and data warehouses, including the BSA Direct system, allow users to more efficiently exploit the data, no system can effectively cull defensively-filed reports. Without a review of underlying supporting documentation, it is often impossible to

determine from a review of a suspicious activity report that it has been filed on events or transactions that are not suspicious. Moreover, we are concerned that as financial institutions spend time and resources on increased filing, the quality of reporting on truly suspicious activity will degrade.

It is no great insight to conclude that the conception of a single, clear policy on suspicious activity reporting, combined with consistency in the application of that policy, is the key solution to the defensive filing phenomenon. Addressing the defensive filing phenomenon, like the other important Bank Secrecy Act compliance issues, is our responsibility. We must issue more and better guidance, adding clarity to the requirements for reporting suspicious activity. We must also work with the federal and state regulatory agencies that examine for Bank Secrecy Act compliance to ensure better that all are examining to achieve proper compliance that is consistent with the goals of the Bank Secrecy Act. I reaffirm my pledge to continue to work closely with the industry and all others to ensure the consistent application of the suspicious activity reporting regulation.

The recent situation involving the termination of certain "high-risk" accounts is also a vexing problem. What has happened to the money services business sector provides an important illustration. It is long-standing Treasury policy that a transparent, well-regulated money services business sector is vital to the health of the world's economy. It is important that all sectors of the financial industry comply with the requirements of the Bank Secrecy Act and applicable state laws, and that they remain within the formal financial sector and subject to appropriate anti-money laundering controls. Equally as important is ensuring that the services provided by money services businesses are subject to the same level of transparency, including the implementation of a full range of controls as required by law. If account relationships are terminated on a widespread basis, we believe many of those who use these services could go "underground" and this potential loss of transparency would, in our view, significantly damage our collective efforts to protect the U.S. financial system from money laundering and other financial crime – including terrorist financing. Clearly, resolving this issue is critical to our achieving the goals of the Bank Secrecy Act.

We have already taken both immediate and longer-term steps to better ensure that money services businesses that comply with the law have appropriate access to banking services. The first step was to eliminate the confusion that had arisen concerning the view of the Financial Crimes Enforcement Network and the Federal Banking Agencies concerning the importance of providing banking services to money services businesses that comply with the law. On March 30, 2005, we issued, jointly with the Federal Banking Agencies, a statement on providing banking services to money services businesses. The purpose of the joint statement was to assert clearly that the Bank Secrecy Act does not require, and neither the Federal Banking Agencies nor we expect, banking institutions to serve as *de facto* regulators of the money services business industry. The joint statement also made it clear that banking organizations that open or maintain accounts for money services businesses are expected to apply the requirements of the

Bank Secrecy Act to money services business customers on a risk-assessed basis, as they would for any other customer, taking into account the products and services offered and the individual circumstances.

The specific interpretive guidance to banks followed a few weeks later. Once again, jointly with the federal banking agencies, we issued guidance that outlined with specificity the minimum anti-money laundering controls banks should apply to money services businesses, risk factors associated with certain money services activity, and requirements for filing suspicious activity reports in connection with money services businesses. We believe that this guidance is a significant step forward, not only for the specific issue of money services businesses securing access to banking services, but also for a model of how we can identify and react to Bank Secrecy Act compliance issues, working closely with the federal regulators.

The money services businesses issue also underscores the need for uniform Bank Secrecy Act examination procedures. To that end, we are working together with the Federal Banking Agencies to develop a set of examination procedures for Bank Secrecy Act compliance. We expect to roll out the procedures this summer, along with an aggressive education and outreach campaign. Moreover, we have already begun joint examiner training through a partnership with the Federal Financial Institutions Examination Council that will provide a forum to provide consistent training related to the conduct of examination procedures.

I am also pleased to announce that we are moving forward on an initiative to enhance our coordination with state level regulatory authorities. Working closely with the Conference of State Bank Supervisors, we have developed a model information sharing agreement that we are seeking to execute with regulatory authorities in the various states that conduct examinations for Bank Secrecy Act compliance. As noted earlier, last month, the State Banking Department of New York became the first signatory to such an agreement, reaffirming their commitment to ensuring the uniform application of the Bank Secrecy Act. We are working with many states now to execute similar agreements and hope to complete this process as soon as we are able.

Finally, we are developing a series of free training seminars for industry, regulators, and law enforcement that will undertake many of the issues that are currently vexing all interested parties. Again, we believe that the successful implementation of the Bank Secrecy Act begins with ensuring that we have taken the time necessary to reach the whole of the financial industry.

Coordination among the regulators, industry, and law enforcement is the lynchpin of effective Bank Secrecy Act compliance. We view this as our responsibility as the administrator of the Bank Secrecy Act. We believe this kind of coordination will help clarify the Bank Secrecy Act requirements and supervisory expectations. While we are not so naïve as to believe that these efforts will solve all issues, we are committed to continue to work with the Federal Banking Agencies and our other federal and state

partners to do everything we can as responsible and responsive regulators, to issue guidance, clarify expectations, and answer questions.

Perhaps the best outcome of the events of late has been the express recognition of the need for all the stakeholders in the Bank Secrecy Act arena to work more closely together to reach our collective goals in a consistent manner. We are working closer with the regulatory agencies than ever before. Not only are we issuing joint guidance and developing uniform examination procedures, but we also are sharing information in a deeper and broader way, as well as developing synergies to the benefit of the regulatory regime as a whole. We are also working more closely with law enforcement. For example, we have formed an interagency working group that brings together regulators and law enforcement to work collectively to identify and address money services businesses that may not be complying with the law and regulations. We have entered into a very productive dialogue with the Department of Justice that will ensure better coordination. Finally, we are setting the stage by building platforms, systems and technologies such as BSA Direct that will allow us to leverage information in a way that we never have before.

Madam Chairwoman, Congressman Gutierrez, distinguished members of the Committee, the importance of your personal and direct support of these efforts cannot be overstated. Your oversight will ensure that we meet the challenges that we are facing. I know how critical it is that we do so and we hope you know how committed we are to meeting those challenges. Thank you.