

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

Good morning Chairman Souder, Ranking Member Cummings, and distinguished members of the Subcommittee. It is a privilege to appear before you to discuss FinCEN's role in terrorist financing and money laundering investigations. I am Robert Werner, Chief of Staff of the Financial Crimes Enforcement Network (FinCEN). Prior to assuming the position of Chief of Staff at FinCEN, I was the Counselor to the General Counsel of Treasury. I have also worked for the United States Department of Justice, as both a federal prosecutor in the District of Connecticut and as an advisor in DOJ's Office of Legal Counsel, concentrating in the areas of administrative and criminal law and criminal procedure.

Background

Since its establishment in 1990, FinCEN has been a service-oriented, information sharing agency dedicated to collecting, analyzing and disseminating financial data to help identify and trace the financial intersection of potential criminal and terrorist activity. Providing this information to our law enforcement, regulatory and financial services partners in appropriate and technologically advanced ways through the FinCEN network is at the heart of FinCEN's mandate to safeguard the U.S. financial system from abuses imposed by criminals and terrorists. Through our role as the administrator of the Bank Secrecy Act (BSA), the regulatory foundation of the nation's anti-money laundering infrastructure, FinCEN adds value to the BSA data to support law enforcement through investigatory leads, trends and pattern information, and to provide financial institutions with feedback on the reports they file. My testimony today will focus on how we carry out our mission and the challenges we are facing going forward.

FinCEN works to accomplish its mission in four principle ways: (1) administration of the Bank Secrecy Act; (2) information collection, maintenance, analysis and dissemination; (3) support to law enforcement; and, (4) networking.

I. Administering the Bank Secrecy Act

The BSA provides the framework within which financial institutions report information relevant to the prevention and detection of criminal activity, including terrorist financing. We work with the various sectors of this broadly defined community,

as well as the functional regulators and the Internal Revenue Service, to ensure that our understanding of sector-specific vulnerabilities is consistent with the objectives of the BSA regulations, and that the affected institutions are in compliance with their reporting obligations. Our financial industry partners include over 20,000 depository institutions, such as banks and credit unions; and over 225,000 non-bank financial institutions such as casinos, broker dealers, money transmitters, check cashers, money order and travelers check businesses, currency exchangers and the U.S. Postal Service. In 2001, the USA PATRIOT Act accelerated the deadlines for the expansion of various BSA requirements to include mutual fund operators, futures commission merchants, the insurance industry, dealers in precious stones and metals, and others.

The success of our regulatory regime is contingent upon open channels of communication. This includes identifying and analyzing the latest trends in money laundering or the financing of terrorism, evaluating the operation of the regulations within each industry, ensuring that necessary information is collected, and providing filing feedback and guidance on compliance.

Hand-in-hand with maintaining a two-way dialogue is the responsibility of FinCEN to educate the financial community about our regulations and expectations concerning their BSA obligations. One area of particular focus is the money services businesses or MSBs. FinCEN has devoted substantial resources to promote MSB compliance with the BSA. In fact, FinCEN has an entire website devoted to MSB compliance obligations (www.msb.gov) and has provided brochures and pamphlets on compliance to MSBs across the nation. However, MSBs continue to require more attention and resources, and FinCEN is undertaking an initiative to educate segments of the industry considered most vulnerable to terrorist abuse.

Each aspect of our regulatory program is designed to ultimately help make the information we provide to law enforcement more valuable in building an investigatory picture.

II. Information Collection, Maintenance, Analysis and Dissemination

While the comprehensive administration of the BSA establishes the guiding framework for the type of information institutions must report, FinCEN must ensure that this information is collected, processed, analyzed and disseminated in a timely manner to its law enforcement partners. We achieve some of this data management with the help of the Internal Revenue Service's Detroit Computing Center. FinCEN's analysts add substantive value to the data by exploiting it tactically and strategically, which I will discuss later in my testimony.

Because information sharing is so critical to our collective efforts to detect and thwart criminal activity, it is necessary to ensure that our data are readily accessible to law enforcement using technology, which is sufficiently advanced to achieve this objective.

Currently, our data are accessed by most of our law enforcement customers through an outmoded data retrieval system linked to the national BSA database at the IRS Detroit Computing Center. Using its tax form processing mission and capabilities, IRS has done a tremendous job over the years as a collection point for the different BSA forms and modes of filing them. But this system does not provide users with the robust data mining capabilities or analytical tools we employ at FinCEN. A signature service of FinCEN, throughout its history, is to continually improve existing and/or develop new programs to enable law enforcement agents in the field to rapidly access the data on-line and to conduct more sophisticated searches of that data. In the absence of these more advanced capabilities, many of our customers are asking for wholesale copies of, or direct access to the data in a way that will not permit us to perform our responsibilities relating to the administration and management of the BSA. Accordingly, we are presently working on a new way for law enforcement to access our databases, called BSA Direct. When fully implemented, BSA Direct will provide law enforcement officials with user-friendly access to our data and robust, state-of-the-art, data mining capabilities that they can use from their own computers. Also, BSA Direct will give FinCEN the time and resources needed to provide more in-depth, analytical support to law enforcement.

Again, in the interest of collecting BSA data rapidly and accurately, we are working to enhance our technological interaction with the financial services industry. Under tight deadlines mandated by the USA PATRIOT Act, FinCEN developed and brought on-line the Patriot Act Communications System, a system that permits the electronic filing of reports required under the Bank Secrecy Act. When financial institutions file their forms on-line through this system, we all benefit. We can provide information to law enforcement more efficiently and accurately. We are working with the financial services industry to encourage more participation in the electronic filing of BSA forms. Our goal is to convert the top 1,500 filers of BSA forms to E-filing over the next 5 – 10 years. Achieving this goal will mean that 90% of all BSA forms will be filed electronically.

III. Law Enforcement Support

Although FinCEN examines its data in support of a wide range of criminal investigations, its top operational priority is unquestionably counter-terrorism support to the law enforcement and intelligence communities. We make our information, products and services available to all agencies that have a role in investigating or analyzing terrorist-related activity and information, including the Terrorist Threat Integration Center (TTIC), the FBI-Terrorist Finance Operation Section, DHS' Operation Cornerstone, the Organized Crime Drug Enforcement Task Force, including its Fusion Center, and other relevant law enforcement entities.

One of the first actions FinCEN undertook following September 11th was the establishment of a Financial Institution Hotline to provide financial institutions with an expedited means of vetting suspicious financial activity possibly linked to terrorism. The financial institution may decide to file a Suspicious Activity Report through the formal

BSA filing process, but the Hotline makes it possible to quickly assess the value of the information and get it into the hands of law enforcement well in advance of normal time constraints associated with the formal process. Since its inception in September 2001, the Hotline has fielded 1,347 calls, 857 of which have resulted in immediate referrals of the information to law enforcement.

At the tactical level, we are implementing a program in which every report that indicates a connection to terrorism is immediately reviewed and validated and then analyzed with other available information to assist law enforcement in “connecting the dots.” These review packages are then immediately referred to TTIC and other terrorism task forces as indicated above.

This program has already produced results. On April 21, 2004, a bank in North Carolina contacted FinCEN’s Financial Institutions Hotline regarding a person who had been a customer since 1999. This person had maintained an average balance of \$1,200 to \$1,500 until very recently, when a total of \$84,000 was deposited in less than a week. Through the analysis of FinCEN’s multiple databases, it was discovered that law enforcement authorities wanted the person as a “deportable felon.” This information was immediately turned over to the appropriate law enforcement agency to act upon, as it deemed best.

Strategically, FinCEN is working to expeditiously enhance the quality of its analysis. As a general matter, Director William Fox has made the training of FinCEN personnel the highest human resource management priority. The top priority of this new program will be analytic skill development relating to terrorist financing. This initiative is intended to build a foundation for continuous improvement of our analytic assets through cross training and diversification, production of joint terrorist financing threat assessments and other reports, and understanding of intelligence processes, the international context of terrorist financing, and the financial industry perspective. In addition, we intend to support training focused on financial forensics, language skills, and geographically targeted studies that focus on culture, infrastructure and other unique aspects of a particular region.

We have adjusted our analytic methodology from a reactive approach to a proactive, think tank environment that will focus on the ways in which terrorist groups move money. To that end, a pilot is underway to look at some of the top-known foreign terrorist organizations through a financial lens. Three analysts are conducting extensive research to study the business models of these organizations. The objective of each analyst is to become familiar with the mechanisms each group uses to eventually be able to identify inherent vulnerabilities in the organization’s business structure.

Through FinCEN’s membership in the Egmont Group of Financial Intelligence Units, which now number 84 worldwide, a bilateral study with our Italian counterpart is going to be conducted to track illicit currency flows between our two countries. This will be the first collaborative effort with a foreign financial intelligence unit on a strategic

project. It is anticipated that this project will be the foundation for additional collaborative efforts amongst the members of this dynamic international network.

Another effort that we at FinCEN are focusing on is the new payment systems such as digital currency businesses, electronic benefit transfer cards and the use of e-gold and e-currency.

One emerging trend, which we believe merits closer scrutiny, is commodities-based money laundering. Director Fox recently made a trip to Dubai to participate in the growing dialogue on the potential use of diamonds and other commodities for illicit purposes, including money laundering and terrorist financing. It is important to note that although it does not have criminal investigative authority, FinCEN has the ability to examine a given topic based upon information gleaned through its vast repository of data as well as its close interaction with its extensive network of law enforcement and industry contacts around the globe. We intend to make greater use of these global resources to further develop such information. The challenge we are facing is to ensure that more and better-trained resources are devoted to this important effort. FinCEN also supports the broader range of investigations carried out by the High Intensity Financial Crime Areas (HIFCAs)¹ by detailing analysts schooled in financial analysis and BSA regulations to the New York, Chicago, Los Angeles, San Francisco, San Juan, Puerto Rico HIFCAs as well as the Southwest Border HIFCA in Austin.

Perhaps the best way to understand some of the general support we provide to law enforcement is to describe a few examples of actual case histories showing how law enforcement has used BSA reports from financial institutions in a variety of criminal investigations:

- Eli Tisona, considered one of Israel's top mobsters, was recently sentenced to 19.6 years incarceration on charges that included money laundering and making false bank statements. In this case, the Miami-Dade Police Department through the Florida Department of Law Enforcement asked FinCEN for assistance. Financial queries of our databases listed Bank Secrecy Act reports that included currency transaction reports on the suspect totaling approximately \$42.5 million. The detective assigned to the case said that without the information reports provided by FinCEN, they could not have made their case.
- Money launderers of drug proceeds who owned a travel agency are currently being prosecuted by the U.S. Attorney's office on these and structuring charges. In the investigation, the Massachusetts State Police conducted a review of FinCEN's databases and their findings included literally thousands of various

¹ On October 30, 1998, the Money Laundering and Financial Crimes Strategy Act of 1998 (MLFCSA) became law. The MLFCSA authorizes the Secretary of Treasury, in consultation with the Attorney General, to designate "any geographical area, industry, sector, or institution in the United States in which money laundering and related financial crimes are extensive or present a substantial risk" as a "high-risk money laundering and related financial crimes area," or a HIFCA.

BSA reports, including suspicious activity reports (SARs), currency transaction reports (CTRs), reports of foreign bank accounts (FBARs) and reports of the transportation of currency and monetary instruments (CMIRs).

- The Pennsylvania Office of the Attorney General's Asset Forfeiture and Money Laundering Section requested that FinCEN conduct proactive, targeting research on suspicious activity reports. The information they obtained from the reports helped them initiate a money laundering investigation on two individuals. Unbeknownst to the Asset Forfeiture Office, the Philadelphia Office of the Immigration and Naturalization Service, was interested in the same individuals. FinCEN's alert program put both offices in touch with each other and, ultimately, together they seized assets valued at about \$8.7 million.

FinCEN's own reviews of suspicious activity reports and currency transaction reports from the financial services industry have revealed numerous indicators of illegal activity which FinCEN provides to law enforcement, regulatory agencies, and the financial industry in the form of investigative leads, advisories, threat assessments and the semi-annual *Suspicious Activity Review*. Some examples are:

- Use of personal accounts to facilitate the negotiation of third-party checks followed by outgoing wire transfers;
- Account activity inconsistent with the type of account held by a customer and/or volume of activity anticipated by the filing institution;
- Large volume of deposits of cash, checks, and other types of monetary instruments immediately followed by wire transactions abroad;
- Structured cash transactions through the use of multiple transactors at multiple branches of the financial institution where the suspect account is maintained; and,
- Use of possible shell companies and multiple accounts to facilitate the structuring of cash, deposit of money orders, and the negotiation of third-party checks, followed by wire transfers from the accounts to high risk countries.

IV. Networking

FinCEN's information, products and services are available to all agencies (whether federal, state, or local) that have a role in investigating illicit finance. Networking is an integral part of this service. It extends the value of our data in multiple ways. Our technology, for example, tells us when different agencies are searching the same data, enabling us to put those agencies together thereby avoiding investigative overlap and permitting the agencies to leverage resources and information.

But perhaps the most prominent example of FinCEN's role as a centralized network has been Section 314 of the USA PATRIOT Act. In recognition of its unique

position as a central focal point for financial information, FinCEN was mandated under that Section to facilitate and enhance the flow of information potentially related to terrorist financing and major money laundering. In general, Section 314(a) allows law enforcement to query U.S. financial institutions about suspects, businesses and accounts in major money laundering and terrorism investigations. FinCEN facilitates this interaction by sending law enforcement information requests to thousands of financial institutions (i.e., banks, credit unions, broker dealers in securities, and futures commission merchants) across the country. These financial institutions, in turn, search their records and transactions, and report positive matches back to FinCEN. FinCEN then consolidates the data and provides this “pointer” information to the law enforcement requestor for follow-up through appropriate legal process.

So far, using this new provision, law enforcement has discovered over 1,000 items of new financial information resulting in over 500 subpoenas, and other legal process to obtain the documentation for these matches. There have already been some arrests and indictments. That’s a pretty impressive success story. We are working to enhance this system further, particularly in our counter-terrorism efforts. Specifically, our analysts are running all 314(a) terrorism-related requests against Bank Secrecy Act data concurrent with these requests being sent to financial institutions. Based on this initial data review, the law enforcement requester is now able to request a more in-depth analysis if desired. The attached illustration of a 314(a) request demonstrates the effectiveness of this system, which enables a law enforcement requestor to instantly canvass the universe of more than 20,000 depository institutions throughout the country to obtain subject match verification.

International Program

A key dimension of the FinCEN network is its global reach. Transnational crime cannot be successfully confronted without building alliances within the global community. Finance today knows no borders. A big part of Title III of the USA PATRIOT Act is dedicated to protecting the international gateways to the United States financial system. But beyond that, FinCEN is committed to improving our international coordination with other countries to support law enforcement in tracking the global financial activities of criminals and terrorists. Law enforcement officials are now able to come to FinCEN to request assistance from our international counterparts, the financial intelligence units of 84 countries throughout the world. Together, we compose a global network called the Egmont Group and we work to improve international information sharing and interaction. In fact, we are implementing a program where FinCEN will automatically request information from relevant financial intelligence unit counterparts as part of any terrorism-related, analysis project.

In addition to our Egmont activities and tied closely to FinCEN’s overall training and technical assistance activities in the international arena is implementation of the U.S. anti-money laundering foreign assistance program, which focuses sharply on terrorist financing. Shortly after September 11, 2001, the Departments of State, Justice, and Treasury convened an interagency group, the Terrorist Financing Working Group

(TFWG), to identify those countries most vulnerable to terrorist financing and to devise a strategy to provide them with the necessary training and technical assistance to create comprehensive, effective anti-money laundering/anti-terrorist financing regimes. FinCEN's International Coordination Group devotes 70% of its time and resources to focusing on those 41 countries.

Challenges in Information Sharing

FinCEN faces many challenges in enhancing information sharing with our law enforcement customers. We feel confident in the steps we are taking in our counter-terrorism strategy, our analytical initiatives, and our enhancements to technology and our international program. However, there is one area of information sharing where we are tentative, and that is in the feedback we can provide to our partners in the financial services industry. FinCEN's regulations require financial institutions to evaluate their vulnerabilities to money laundering and terrorist financing. Maybe most importantly, the regulator under a risk-based system must find an appropriate way to provide the regulated industry with information necessary to permit the industry to assess the risk. This is not easy. For example, if terrorism is our greatest threat, how does FinCEN appropriately and effectively communicate information that may be relevant, but is classified? Those in law enforcement are correctly reticent about sharing information outside their investigative circles. How do we get relevant information from those investigations to our industries so they can assess their risks? As difficult as this may be, FinCEN must find a way to provide the industries we regulate with information relevant to their assessment of the risk. We are beginning discussions on this gap in information sharing with our industry, law enforcement, and regulatory partners.

I would also note that along with information sharing comes the responsibility of ensuring the protection of that information. FinCEN follows a comprehensive set of legal and technological restrictions to ensure its data are properly used internally as well as externally. Such controls are designed to compartmentalize and channel information only to authorized users to ensure compliance with U.S. privacy laws. Unauthorized disclosures have been extremely rare and are immediately referred to law enforcement for investigation and dealt with as severely as the law permits.

Conclusion

FinCEN, its network and its mission are dedicated to fostering a dynamic information-sharing environment among its law enforcement, regulatory and financial partners. The agency will continue to build upon its expertise and add the benefit of its successes and lessons learned to the nation's anti-terrorism and money laundering efforts. Thank you again for this opportunity to testify today on FinCEN's role in terrorist financing and money laundering investigations. I would be happy to answer any questions the Subcommittee may have.